ASISA
Association for
Savings & Investment
South Africa

ASISA GUIDELINE ON INFORMATION SHARING (FRAUD AND OTHER UNLAWFUL ACTS)

Date of first publication: March 2026

Date of last update:

1. INTRODUCTION

1.1. Collaboration and the sharing of data and intelligence is widely accepted as the best method of combatting fraud, scams and other misconduct. Leveraging fraud intelligence enables organisations to build more reliable and robust fraud defences and to act on accurate insights to stop fraud before funds disappear.

1.2. No single organisation can see the full picture of a fraud network. Transactions that look legitimate in one institution might look suspicious when viewed across multiple institutions. Without collaboration and intelligence sharing, these patterns remain hidden.

1.3. Intelligence sharing allows organisations to move from reactive fraud detection to proactive prevention, reducing financial losses and protecting customers.

1.4. Notwithstanding these benefits, ASISA members ("**Members**") may be reluctant to explore data sharing due to concerns over data privacy and compliance – particularly around information that can and cannot be shared, and the liabilities attached to disclosure.

1.5. On 18 July 2024, ASISA published a **Guideline on Sharing Information** under the auspices of the Forensic Standing Committee. It has subsequently transpired that there is a need for additional guidance to Members on the sharing of personal information relating to fraud and other unlawful activities amongst one another, including on the topic of insurance claims fraud.

1.6. This **Guideline on Sharing of Information (Fraud and Other Unlawful Acts)** ("**Guideline**") has accordingly been prepared in an effort to provide more detailed guidance to Members regarding the lawful sharing of information with one another to support fraud and other unlawful conduct detection and mitigation efforts and to assist Members to carry out this information sharing in a responsible, fair and a proportionate way. This Guideline replaces the previous Guideline on Sharing Information.

1.7. This Guideline is being shared with Members and the public at large for their consideration and voluntary implementation and is non-binding on Members. Members should take their own decisions as to how they will use this Guideline.

1.8. Please note that the material and information contained in this Guideline are for general information use and do not constitute legal advice.

2. PROTECTION OF PERSONAL INFORMATION

2.1. The Protection of Personal Information Act ("**POPIA**") regulates the processing (which includes sharing) of personal information in South Africa. Importantly, POPIA does not prevent an organisation from sharing personal information where it is appropriate to do so, or from taking steps to prevent harm.

2.2. The concepts of necessity and proportionality are fundamental principles under POPIA:

2.2.1. Necessity requires that any limitation on fundamental rights, such as privacy, must be justified with objective evidence.

2.2.2. Proportionality ensures that the measures taken are appropriate and not excessive in relation to the intended purpose.

Both principles must be satisfied for the lawful processing of personal information, meaning that any processing of personal information must be necessary for a legitimate purpose and proportionate to that purpose.

What is personal information?

2.3. The definition of "*personal information*" in POPIA[1] includes almost all types of information regarding natural or juristic persons.

2.4. To the extent that the information being shared does not relate to the personal information of a

[1] Section 1 of POPIA defines "***personal information***" as "*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."

specific person or the information has been de-identified[2], POPIA will not be applicable.

2.5. In this regard, it should be noted that information is not to be considered personal information for a given entity when it does not have the means to identify the person to whom the information relates with undue effort - the data subject must be identifiable in the hands of the organisation that receives the information. This means that, if a Member shares information with other Members and the other Members cannot, without unreasonable effort, reconstruct the identity of the person from their own data, the information shared will not constitute personal information (even if it is personal information in the hands of the Member who shared the information). In this context, whether information is considered "personal" depends on the perspective and identification capabilities of the party handling it.

2.6. It should also be noted that POPIA does not regulate personal information of a deceased person.

What are the grounds for lawful processing of personal information?

2.7. Section 11 of POPIA provides that personal information may only be lawfully processed on certain grounds, including:

2.7.1. processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied;

2.7.2. processing complies with an obligation imposed by law on the responsible party.

Legitimate interest ground

2.8. The sharing of personal information amongst Members may be justifiable on the legitimate interest basis referred to in paragraph 2.7.1. Legitimate interests can include commercial interests, individual interests or broader societal benefits. Recognised examples include preventing fraud, preventing or detecting a crime and preventing or detecting unlawful acts. Members have a vested financial interest in mitigating these risks.

2.9. The word "*necessary*" in the legitimate interest basis does not mean that the processing of information must be absolutely necessary to achieve the purpose, but that the processing must

[2] Section 1 of POPIA defines "***de-identify***" as "*in relation to personal information of a data subject, means to delete any information that—*
(a) identifies the data subject;
(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject".

be a targeted and proportionate way of achieving the purpose.

2.10. As far as the sharing of information of suspected fraud or other unlawful acts is concerned, there has to be at least a reasonable suspicion of (potential) fraud or other unlawful acts. This means that there must be an objectively justifiable belief, based on specific facts or circumstances that a person is involved in a fraudulent or otherwise unlawful activity.

Guidelines – reasonable suspicion

- Reasonable suspicion exists when an objective person, taking into account the facts and circumstances of a particular situation, would believe that someone was committing fraud or an unlawful act. Section 1(3) of the Prevention of Organised Crime Act provides that a person ought reasonably to have known or suspected a fact if a reasonably diligent and vigilant person with the same knowledge, skill, training and experience, as well as the knowledge, skill, training and experience that may reasonably be expected of a person in the same position, would have known or suspected that fact. The Financial Intelligence Centre Act also uses the phrase "*ought reasonably to have known or suspected*" in section 29(1) that deals with suspicious transactions.

- Reasonable suspicion requires more than a mere hunch or a gut feeling or an early warning indicator (which lacks objective facts or a rational foundation). It demands specific and articulable facts that lead the Member to suspect that a fraudulent or other unlawful activity is occurring or has occurred. These facts must be objective and explainable, ensuring investigations are not arbitrary. The suspicion must be associated with a specific individual, not just a general sense of unease.

- Whatever detection measures or red flags are used by Members to detect potential fraud or unlawful conduct, e.g. initial forensic investigations, third party data base checks, data analysis or artificial intelligence, the Member should aim to only share data with other Members or third parties once there is a reasonable suspicion of fraud or other misconduct.

- This does not mean that Members can't make use of available data bases which already contain data on suspected or confirmed fraud or other misconduct to inform a reasonable suspicion.

- The ordinary meaning of "*reasonable*" is what is in accordance with reason, appropriate, sensible or fair. What is "reasonable" will depend on the facts of the case and the internal processes employed by each Member to identify suspected fraud or misconduct.

- Premature suspicions of fraud or other misconduct can lead to significant legal and other consequences. It is crucial to have a reasonably well-informed and substantiated suspicion before sharing the information.

Examples – reasonable suspicion

Case Study 1:

A member has received a complaint that contains sufficient information to support the complaint and to cause a reasonable belief that unlawful conduct has occurred (a credible complaint).

- This would constitute a reasonable suspicion.

Case Study 2:

A member has a proactive process (rules, machine learning, etc) that assesses transactions and identifies anomalies. The identified anomalies are then reviewed by an analyst and, where the analyst believes that there is a suspicion of unlawful conduct, the matter is further investigated.

- Once the analyst suspects that unlawful conduct may have been committed after analysis, this would amount to a reasonable suspicion of misconduct.

Case Study 3:

A Member follows a proactive process to flag suspicious transactions (e.g. it uses internal rules, models and AI). Upon the flagging of a transaction, the transaction is either stopped or is routed for investigation.

- The mere proactive flagging of a transaction as suspicious through internal controls, is not sufficient to create a reasonable suspicion. There will have to be a further initial investigative or analysis step in the process.

Examples – legitimate interest basis

Case Study 4:

An insurer is suspicious about a claim it is assessing and knows the life insured has cover elsewhere in the market (for example having conducted checks on an industry database). May the insurer share information with and obtain information from the other insurers with which the life insured holds cover if it hasn't confirmed yet that fraud has been perpetrated?

- POPIA allows for certain circumstances in which the sharing of information is allowed without consent, such as when the sharing is necessary for purposes of a legitimate interest of the responsible party or a third party. Legitimate interests include preventing

or detecting fraud, crime or other unlawful acts.

- The insurer may accordingly lawfully share this information with other insurers to establish whether fraud, crime or an unlawful act has been committed and to prevent further harm.

- The suspicion of fraud or other misconduct will be sufficient to share the information – the fraud or misconduct does not have to be confirmed. However, the insurer would have to be able to demonstrate that there is a reasonable suspicion of fraud.

If the insurer does confirm fraud, is there any obligation to notify other insurers that have cover for the insured?

- There is currently no law that requires such notification. However, in the spirit of collaborative fraud prevention, it would be good practice to do so.

Would insurers have to get consent from or notify the suspect that they are under investigation? Do they have to reveal their source of information to the suspect.

- Consent is not required as the insurer is relying on a different processing ground.

- There is no obligation in terms of POPIA to provide this kind of information to the suspect. In fact, notification to the suspect of a specific investigation or revealing the source of information to the suspect will likely impede the investigation, for example if evidence is destroyed, and will defeat the whole purpose for the processing of the information. Regard must also be had to the provisions of section 29 of the Financial Intelligence Centre Act which prohibits tipping off the suspect.

- However, the insurer should include a general statement in their section 18 Privacy Notices that they may process personal information for purposes of detecting and preventing fraud or other unlawful conduct (see section on **Notification Obligations** below).

Does fraud cover material misrepresentation?

- Material misrepresentation may constitute fraud, but it will not always. Fraud may be related to misrepresentation, but it could also involve other types of misconduct.

- "**Fraud**" can be broadly defined as an intentionally deceptive action to provide the perpetrator with an unlawful gain and/or create a loss for or deny a right for another.

- "**Misrepresentation**" can be broadly described as a false representation made verbally, in writing or by conduct or concealment and for the purposes of deceiving, defrauding or causing another to rely on it detrimentally, including to deliberately state information or facts in a wrongful or misleading way. ASISA is in the process of finalising the **ASISA Guideline on Misrepresentation and Non-Disclosure** which aims to assist Members in this regard.

- Even if the perpetrator's actions do not constitute fraud, the insurer can still rely on the legitimate interest processing ground that it is detecting or preventing unlawful acts, such as misrepresentation.

If individual insurers agree that fraud is potentially concerned and wish to investigate, should each insurer conduct their own investigations or may they work collaboratively?

- Each insurer should follow their own internal processes for fraud investigations. If more than one insurer is involved, they should decide amongst themselves what information they want to share or if they want to outsource the investigation to the same or different third parties. Suspicions of fraud would also have to be reported to SAPS or other fraud prevention bodies.[3]

Case Study 5:

In executing the mandate of the ASISA Forensics Standing Committee, Members who are part of that committee wish to share information amongst one another in an effort to prevent and detect fraud. The information may include personal information. The sharing mostly happens via telegram messaging or WhatsApp. May this be lawfully done?

- The sharing of information between Members in the context of investigating claims fraud or scams is crucial. Without that exchange of information, a fraud investigation can be substantially impeded.

- As mentioned above, the investigation, detection or prevention of fraud, scams or other misconduct is a recognised legitimate interest. If sharing personal information in these circumstances, Members should look at legitimate interests as a lawful basis because of the compelling justification of preventing harm.

- It is recommended that a robust assessment is done of whether sharing specific types and categories of personal information is necessary and that it is a targeted and proportionate way of preventing harm that cannot be reasonably achieved in another less intrusive way.

Obligation in law

2.11. Another lawful processing ground on which Members may be able to rely is the obligation in

[3] In South Africa, individuals who have reasonable grounds to suspect fraud must report it to the SAPS. This is a statutory duty under the Prevention and Combating of Corrupt Activities Act. This Act requires that any person who holds a position of authority and knows or suspects that another person has committed and offence related

law basis referred to in paragraph 2.7.22.7.1. This is, in short, when a Member shares personal information to comply with or give effect to the law.

2.12. This does not mean that there must be a legal obligation specifically requiring the specific processing activity (sharing). The point is that the Member's overall purpose must be to comply with or give effect to a legal obligation which has a sufficiently clear basis in either common law or statute.

2.13. In the context of insurers, GOI[4] 3 Risk Management and Internal Controls for Insurers ("**GOI 3**") requires insurers to have a board approved policy to deal with insurance fraud. Such a policy must:

2.13.1. outline appropriate strategies, procedures and controls to deter, prevent, detect, report and remedy insurance fraud;

2.13.2. outline appropriate strategies for managing fraud risk and the risk to the insurer's financial soundness or sustainability caused by fraud;

2.13.3. take into consideration how the effectiveness of fraud risk management may be enhanced by contributing to industry-wide initiatives to deter, prevent, detect, report, and remedy insurance fraud;

2.13.4. provide for the prompt reporting of insurance fraud to relevant regulatory authorities.

From the wording of GOI 3 it can only be inferred that insurers should address potential fraud internally and at an industry level.

2.14. In cases of cyber security incidents, the Joint Standard 2 of 2024 issued by the Prudential Regulator and the Financial Sector Conduct Authority entitled "*Cybersecurity and Cyber Resilience Requirements*" ("**Cyber Standard**") may also be relied upon. In this regard, the Cyber Standard provides[5] that financial institutions must participate in cyber threat information-sharing arrangements with trusted external parties to (a) share reliable, actionable cybersecurity information regarding threats, vulnerabilities, and incidents to enhance defences; and (b) receive timely and actionable cyber threat information.

---

to fraud must report this knowledge or suspicion to a police official. Failure to report such suspicions is also considered an offence.

[4] Governance and Operational Standards for Insurers.

[5] Paragraph 7.6.2(a)(iii) of the Cyber Standard.

2.15. As with the legitimate interest basis, although the processing need not be essential to comply with the legal obligation, it must be a reasonable and proportionate way of achieving compliance. A Member should not rely on this lawful basis if the Member has discretion over whether to process the personal information, or if there is another reasonable way to comply.

Examples – Obligation in law

Case Study 6:

ASISA Members want to address fraud at an industry level and want to proceed with an industry wide initiative to share information on fraudulent or other unlawful cases in an effort to prevent and detect insurance fraud. Does POPIA permit such sharing of information?

- POPIA provides that personal information may be shared in order to comply with an obligation imposed by law on the responsible party.
- GOI 3 provides that insurers must take into consideration how the effectiveness of fraud risk management may be enhanced by contributing to industry-wide initiatives to deter, prevent, detect, report, and remedy insurance fraud.
- ASISA Members would be able to rely on the obligation imposed by GOI 3 to share fraud related information for purposes of an industry initiative.

Case study 7:

ASISA members wish to share with one another critical information about cyberattacks and vulnerabilities to plan, process, and develop cybersecurity measures. That's because one organization alone can't identify and mitigate all cyber-attacks. There is also an obligation on Members under the Cyber Standard to share cyber threat information to enhance defences.

- Members would be able to rely on the obligation imposed by the Cyber Standard to share information on cyberattacks and cyber threats with trusted external parties.

Member responsibilities

2.16. It is up to each Member to:

2.16.1. determine which processing ground is most appropriate to rely on for the sharing of information relating to (potential) fraud and misconduct;

2.16.2. control the management of such sharing of information and ensure compliance with POPIA.

3. SPECIAL PERSONAL INFORMATION

3.1. In terms of POPIA, certain information constitutes special personal information that merits special protection, e.g. information regarding **race or ethnic origin**, **health** or sex life and **criminal behaviour** to the extent that such information relates to:

3.1.1. the alleged commission by a data subject of any offence; or

3.1.2. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.[6]

3.2. Although Members may accordingly establish a lawful processing ground, POPIA prescribes that special personal information may only be processed (shared) without consent in very limited circumstances, including that:

3.2.1. Processing is necessary for the establishment, exercise or defence of a right or obligation in law. [7]

3.2.2. Information has deliberately been made public by the data subject. [8]

3.2.3. In the case of **race or ethnic origin** information, processing is carried out to:

3.2.3.1. identify data subjects and only when this is essential for that purpose; and

3.2.3.2. comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.[9]

3.2.4. In the case of **health information**, if such processing is necessary for:

3.2.4.1. assessing the risk to be insured by the insurance company and the data subject has not objected to the processing;

---

[6] POPIA creates a distinction between that of 'criminal information' and 'criminal behaviour'. 'While processing "criminal information" does not require consent, processing "criminal behaviour" falls under special personal information. Criminal information' is defined within 'personal information' and refers to the criminal history of a person, such as criminal and background checks. Special personal information includes, among others, screening records relating to criminal convictions.

[7] See section 27 of POPIA.

[8] See section 27 of POPIA.

[9] See section 29 of POPIA.

3.2.4.2. the performance of an insurance agreement; or

3.2.4.3. the enforcement of any contractual rights and obligations; [10]

3.2.5. In the case of information relating to **criminal behaviour**:

3.2.5.1. if the processing is carried out by bodies charged by law with applying criminal law or by persons who have obtained that information in accordance with the law;

3.2.5.2. if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information permitted by law. [11]

Examples – special personal information

Case Study 8:

A Member suspects that fraudulent documents have been submitted in the course of a claim. The Member thinks that the policyholder also holds a policy with another Member, but is not certain and would like to cross-check the identity of the policyholder with the other Member. As part of the check, the Member would like to confirm the race of the policyholder.

- The race of the policyholder is special personal information under POPIA. In this case, although the sharing of personal information can be justified on the legitimate interest ground, the Member will have to meet one of the conditions set out for processing personal information.
- In this case, confirming the race is not necessary for the establishment, exercise or defence of a right or obligation in law.
- Although the Member would like to confirm the identity of the policyholder, it is not doing so in order to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.
- Less intrusive measures may be used to confirm the identity of the policyholder, such as using full names and identity number.
- The Member would not be permitted under POPIA to share details of the policyholder's race with the other Member.

Case Study 9:

[10] See section 32 of POPIA.

[11] See section 33 of POPIA.

A Member receives a disability claim, but suspects that the claim is false. The Member is aware that the policyholder also holds disability cover with another Member and would like to check with the other Member if that Members has also received a claim. For this purpose, the Member needs to share information on the disability event, which includes health information.

- Health information is special personal information and the processing thereof will have to meet the stricter requirements set out in POPIA.
- The aim of sharing the information with the other Member is largely to inform a claim decision.
- The Member should be able to rely on the condition that the sharing of health information is done in order to assist the Member in making a decision as to how to enforce its contractual rights or obligations under the policy contract (e.g. to pay out, refuse the claim or even repudiate the policy contract).

Case Study 10:

A Member wishes to conduct a criminal check on a claimant suspected of being involved in an insurance scam to obtain the claimant's criminal history. For this, the Member makes use of a background check service provider. The Member is also aware that the claimant has been accused of a crime and is currently awaiting trial. Which information can the Member rely on to investigate the claimant?

- A distinction must be made between information that refers to criminal behaviour and information that refers to criminal history.
- Criminal behaviour refers to the information of a person who has only been accused of a criminal act, but not yet convicted by a competent court. This falls under the definition of special personal information and in terms of POPIA may not be processed without the consent of the person whose information it is.
- Criminal history, on the other hand, refers to information of an individual who has already been convicted in a competent court and therefore such information has become public knowledge and may be processed as such in terms of POPIA.
- The Member may accordingly rely on the information obtained from the service provider regarding the claimant's personal history (if any). The Member may rely on the legitimate interest ground to collect such information. However, the Member would not be able to rely on the information about the claimant's current alleged crime, as the Member is not a person charged by law with applying criminal law and the information will constitute information about criminal behaviour.

4. CYBERCRIME

4.1. As with fraud, the processing of personal information for the prevention, detection or investigation of crimes (including cybercrime), including the apprehension and prosecution of offenders, can also be justified on the legitimate interest processing ground. These purposes are activities in the public interest - protecting people from harm and serves the interest of society at large - and any potential impact on people could therefore be justified – subject to other data protection considerations as normal.

4.2. Members may also rely on the ground that information sharing is justified in order to comply with an obligation imposed on them by law. As mentioned above, the Cyber Standard enjoins Members to share information on cyber threats and attacks in order to enhance defences and receive timely and actionable cyber threat information.

Examples - Cybercrime

Case Study 11:

An insurance company wants to use personal information to spot fraudulent claims and recover money it has paid out on dishonest claims.

- The insurer may rely on the legitimate interest ground of detecting, investigating or prosecuting a crime to handle personal information in this way.
- To ensure its use of personal information is targeted and proportionate, the insurer should follow industry best practice when deciding what fraud indicators to look for in new claims so that these can be reviewed further by its fraud investigation team.

Case Study 12:

The ASISA/SAIA-CSIRT co-ordinates responses to cyber and information security incidents experienced by ASISA and SAIA members. It also provides cyber threat related information to members, to reduce the risk of cyber security incidents to their individual businesses. As part of their mandate, members share indicators of compromise and incident related information, for example through Telegram. This could assist the other CSIRT members to identify a potential compromise early and to limit the potential impact, or to prevent a compromise from happening. This also enables the CSIRT to quickly assess whether an attack is focussed on a specific business, the industry, region or whether it is a high volume 'un-focussed' attack.

- It is clear that the sharing of perpetrator or even customer information is done in order to detect cyber and other crimes. As such, both the Members sharing the information and the Members receiving the information are able to rely on the legitimate interest processing ground of crime detection and prevention.
- Members may also rely on the ground that information sharing is justified in order to

comply with an obligation imposed on them by the Cyber Standard.

5. JOINT RESPONSIBLE PARTIES

5.1. A ‘‘**responsible party**’’ is defined in POPIA as any “person which, alone or in conjunction with others, determines the **purpose of and means** for processing personal information”.

5.2. When responsible parties decide the purposes and means of processing together, e.g. the sharing of information for purposes of fraud prevention, they are joint responsible parties. This will include data pooling where responsible parties decide to pool information they hold together and make it available to one another for a specific purpose.

5.3. Even if Members are seen as joint responsible parties, and regardless of the data sharing arrangements between Members, each Member remains responsible for complying with all the obligations of responsible parties under POPIA and accountable to the Information Regulator.

6. OTHER PROCESSING CONDITIONS

6.1. Even where a lawful ground for processing exists, Members still have to comply with the other conditions of lawful processing set out in POPIA to ensure that this is done in compliance with the law.[12] For detailed guidance, Members are referred to the **ASISA Guideline for Processing Personal Information**.

Data subject notification obligation

6.2. Importantly, although consent may not be required to share information, section 18 of POPIA requires responsible parties to take reasonable steps to notify the persons whose data is being processed about certain aspects of the processing, including:

6.2.1. the information being collected and where the information is collected from;

6.2.2. the purpose for which the information is being collected;

6.2.3. any particular law authorising or requiring the collection of the information;

6.2.4. any further information such as the:

[12] Section 8 of POPIA provides that: “*The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself*.”

6.2.4.1. recipient or category of recipients of the information;

6.2.4.2. nature or category of the information.

6.3. The notification must be provided:

6.3.1. 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

6.3.2. in any other case, before the information is collected or as soon as reasonably practicable after it has been collected. [13]

6.4. In some instances, it is not necessary to provide the data subject with the notification, including where:

6.4.1. compliance would prejudice a lawful purpose of the collection – in this case notification of the processing of information is likely to prejudice the detection, investigation and prevention of unlawful activities;

6.4.2. compliance is not reasonably practicable in the circumstances of the particular case.[14]

Guidelines – data subject notification

- Section 18 of POPIA only deals with **notification** requirements, not consent. Unless consent is relied on as the lawful processing ground, consent for the processing does not have to be obtained. Data subjects must simply be notified of the items listed in section 18.
- The easiest way to notify data subjects is by way of Members' **Privacy Notices**.
- It is recommended that Members' Privacy Notices contain provisions to the effect that personal information may be collected and further used for the detection, prevention, investigation and combatting of fraud and other unlawful activities, including the sharing of personal information with other Members, on industry data bases and with regulatory or law enforcement authorities.
- It is also recommended that Members include a provision in their Privacy Notices to the effect that health information may be used for purposes of assessing the risk at underwriting and claim stage.

[13] See section 18(2) of POPIA.
[14] See section 18(3) of POPIA.

Example – data subject notification

Case Study 13:

A CSIRT member shares information about a cyber incident of which it has become aware with other CSIRT members. This includes information about the identity of the attacker and the location of the site. Does the CSIRT member or the other members the information is shared with have to notify the perpetrator that its information is being shared?

- The CSIRT members will be able to rely on the exemption of the notification requirements that compliance would prejudice a lawful purpose of the collection. They will accordingly not have to notify the perpetrator.

Minimality

6.5. When sharing personal information, regard must be had to section 10 of POPIA which provides that personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

6.6. If Members accordingly want to share personal information for purposes of preventing fraud or other unlawful activities, they should ensure that only the minimum information required for those purposes is shared. Any sharing that goes beyond this will be unlawful.

Example - minimality

Case Study 14:

A Member wants to add information about a suspected crime to a central data base or warn other members. The information that it wants to share also consists of information that would not be required for other members to investigate possible crimes in their organisation, for example policy numbers and details of policy premiums.

- The Member should only share information that is necessary given the purpose for which the information is being shared. It is not necessary for other members to have details of the policy number or the premium amount to investigate a potential crime on their side. The Member should accordingly delete any unnecessary information from the data it shares with other Members.

Accountability and lawfulness of processing

6.7. Responsible parties are accountable for ensuring that personal information is processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.[15] Members should be able to demonstrate their compliance with this processing condition.

Collection directly from the data subject

6.8. Information must, as far as possible be collected directly from the data subject. Information may be collected from other sources if compliance would prejudice a lawful purpose of the collection or compliance is not reasonably practicable in the circumstances of the particular case.

Guideline – collection directly from the data subject

- In order to detect or prevent fraud or other misconduct, Members may collect personal information from other sources than the data subject, given that collection from the data subject would prejudice the purpose of collection.

Purpose limitation

6.9. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Member.[16] In this case the purpose is the detection, prevention and investigation of fraud and other unlawful activities. Members with whom the information is shared may not use the information for another purpose, unless the new purpose is compatible with the original purpose, they get consent, or they have a clear obligation or function set out in law.[17]

---

[15] See section 9 of POPIA.

[16] See section 13 of POPIA.

[17] Section 13 of POPIA provides that: "*Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party*." Section 14 provides that: "*records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—*

(a) retention of the record is required or authorised by law;

(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject has consented to the retention of the record."

Guideline – purpose limitation

- Using personal information for purposes of preventing fraud or other unlawful activities is not compatible with the original purpose that the information was collected for, e.g. for purposes of concluding or giving effect to an insurance policy. If personal information is going to be used for the former purposes, the customer must be notified. It is accordingly important that Members' Privacy Notices set out all the different purposes that the information may be used for to make sure they are covered.

Record retention

6.10. Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless retention of the record is required or authorised by law or the Member reasonably requires the record for lawful purposes related to its functions or activities.[18]

Destruction

6.11. A Member must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the Member is no longer authorised to retain the record.[19]

Data quality

6.12. Members must take all reasonable steps to ensure the personal information processed is not incorrect or misleading.[20]

Documentation

6.13. Members must maintain documentation of all processing operations under their responsibility.[21]

[18] See section 14(1) of POPIA.

[19] See section 14(4) of POPIA.

[20] Section 16 of POPIA provides that: "*A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary*."

[21] See section 17 of POPIA.

Security

6.14. Members must secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information.[22]

Guidelines - security

- In the sharing and hosting of personal information received from other Members, Members must take reasonable measures to:
    - identify all reasonably foreseeable internal and external risks to personal information in their possession or under their control;
    - establish and maintain appropriate safeguards against the risks identified;
    - regularly verify that the safeguards are effectively implemented; and
    - ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented strategies.
- Members must have due regard to generally accepted information security practices and procedures which may apply to them generally or be required in terms of specific industry or professional rules and regulations.
- Members should take active steps to enhance their cyber security in order to protect the personal information they hold.
- Members should only disclose personal information to their staff on a "need-to-know" basis and should take all reasonable steps to impress upon their staff the Members' obligations under POPIA.

[22] See section 19 of POPIA.

Examples - security

Case Study 15: (UK example)

A malicious file was unintentionally downloaded onto an employee device on 22 March 2023. Despite a high priority security alert being raised within 10 minutes of the breach and some immediate automated action being taken, the organisation did not quarantine the device for 58 hours, during which the attacker was able to exploit its systems.

This file enabled the deployment of malicious software onto the organisation's network, allowing the hacker to stay in the system, gain administrator permissions and access other areas of the network.. Between 29 and 30 March 2023, nearly one terabyte of data was exfiltrated. On 31 March 2023, ransomware was deployed onto the organisation's systems and the hacker reset all user passwords, preventing staff from accessing their systems and network. The Information Commissioner's office (ICO") received at least 93 complaints in relation to this attack.

- The ICO's investigation found that the organisation failed to implement appropriate technical and organisational measures to safeguard the data they held. This included:
    - Failure to prevent privilege escalation and unauthorised lateral movement:
        - The organisation did not implement a tiering model for administrative accounts. This allowed the attacker to escalate privileges, move laterally across multiple domains and compromise critical systems.
        - These failings were flagged as a vulnerability on at least three separate occasions but were not remedied.
    - Failure to respond appropriately to security alerts:
        - A high priority security alert was raised within ten minutes of the breach, but the organisation took 58 hours to respond appropriately, against a target response time of one hour.
        - The organisation's Security Operations Centre was understaffed, and in at least six months before the incident fell well below the target response times for responding to security alerts.
    - Inadequate penetration testing and risk assessment:
        - Systems processing millions of records, including some sensitive data, were only subject to a penetration test upon being commissioned and were not subject to any subsequent penetration test.

    - Findings from penetration tests were siloed within business units. Risks identified that affected the wider organisational network were not universally addressed.

- The ICO and the organisation agreed to a voluntary settlement penalty of £14 million.

Case Study 16

During September 2021, the Department of Justice and Constitutional Development ("DoJ&CD") suffered a security breach on its IT systems, reported as a ransomware attack. This led to the department's systems being unavailable to its employees and subsequently affecting public service and resulting in the loss of approximately 1 204 files. This breach was mainly due to the failure by the department to renew its security incident and event monitoring license, its detection system license and trend antivirus license.

- The Information Regulator conducted an assessment and found that the department had failed to put in place adequate technical measures to monitor and detect unauthorised exfiltration of data from their environment. It was also found that the department failed to take reasonable measures to identify, or reasonably foresee, internal and external risks to the protection of personal information or establish and maintain appropriate safeguards against the identified risk.

- The department was fined R10 million by the Information Regulator, a landmark move in 2023 that highlighted the real cost of non-compliance.

Case Study 17

In March 2022, TransUnion, a registered credit bureau and a repository of credit information on consumers and businesses, submitted a section 22 notification indicating that it had suffered a security compromise. A host of details were stolen, including names, ID numbers, contact details, vehicle finance data and other personal information.

- Following an investigation into the breach, the Information Regulator found that TransUnion violated the conditions for the lawful processing of information by:

    - Failing to secure the confidentiality of personal information in its possession.

    - Failing to take appropriate technical and organisational measures to ensure access control is implemented and also not having controls to detect failures.

    - Failing to prevent unlawful access to or processing of personal information

through the use of compromised credentials and use of a weak password.

- Failing to implement safeguards that had been put in place.
- Failing to implement the provisions of its own information security policies.

- TransUnion was hit with an enforcement notice by the Information Regulator.

Automated decision making

6.15. Please also note that Members must obtain prior authorisation from the Information Regulator[23] prior to any processing if Members plan to process any unique identifiers of data subjects:

6.15.1. for a purpose other than the one for which the identifier was specifically intended at collection; and

6.15.2. with the aim of linking the information together with information processed by other responsible parties. [24]

6.16. A Member will accordingly have to get permission from the Information Regulator if it plans to share unique identifies with other responsible parties in order to link that unique identifier with personal information held by such other responsible parties.

Guidelines

- In terms of POPIA, a ‘‘**unique identifier**’’ means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.
- Examples of unique identifies include identity numbers, telephone numbers, policy numbers and bank account numbers.
- A member only has to obtain prior authorisation from the Information Regulator only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised.

[23] In terms of section 58 of POPIA.
[24] See section 57 of POPIA.

DOCUMENT HISTORY

Date	Publication/amendment
18 July 2024	Publication of the ASISA Guideline on Sharing Information (Forensics Standing Committee)
March 2026	First publication of the ASISA Guideline on Information Sharing (Fraud and Other Unlawful Acts)

RESPONSIBLE SPA AND COMMITTEES

Responsible Board Committees	Life and Risk Board Committee Technical and Operations Board Committee
Responsible Standing Committees	Claims Standing Committee Forensics Standing Committee
Responsible Senior Policy Advisors	ASISA Point Person to the Life and Risk Board Committee ASISA Point Person to the Technical and Operations Board Committee