ASISA GUIDELINE ON SHARING INFORMATION

Date of first publication: 18 July 2024

Date of last update: 18 July 2024

1. INTRODUCTION

1.1. In executing the mandate of the ASISA Forensics Standing Committee, ASISA members who are part of that committee ("**Members**") share information relating to customers and their respective business amongst one another.

1.2. This Guideline on Sharing of Information ("**Guideline**") has been prepared in an effort to provide guidance to Members regarding the most important regulation applicable to the sharing of such information.

2. THE PROTECTION OF PERSONAL INFORMATION

Personal information

2.1. The Protection of Personal Information Act ("**POPIA**") regulates the processing (including the sharing) of personal information. The definition of "*personal information*" in POPIA includes almost all types of information regarding natural or juristic persons.

2.2. To the extent that the information being shared does not relate to the personal information of a specific customer or the customer cannot be identified from such information, POPIA will not be applicable.

Grounds for lawful processing of personal information

2.3. Section 11 of POPIA provides that personal information may only be processed on certain lawful grounds:

2.3.1. the data subject consents to the processing;

2.3.2. processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

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

2.3.4. processing protects a legitimate interest of the data subject;

2.3.5. processing is necessary for the proper performance of a public law duty by a public body; or

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

2.4. The sharing of personal information amongst members may be justifiable on the legitimate interest basis referred to in paragraph 2.3.6. Legitimate interests can include commercial interests, individual interests or broader societal benefits. Recognised examples include preventing fraud, preventing or detecting a crime, preventing or detecting unlawful acts, and being necessary for an insurance purpose (the handling of a claim).

2.5. 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 be a targeted and proportionate way of achieving the purpose.

2.6. The sharing of information between financial institutions, such as insurers, in the context of investigating claims fraud is crucial. Without that exchange of information, a fraud investigation can be limited, particularly in third party claims where no prior relationship between financial institution and claimant exists.

2.7. It is clear therefore that information can be shared for the purpose of investigating fraud by the legitimate reason of detecting a crime or unlawful act. An insurer can also share information lawfully where it is necessary for an insurance purpose.

2.8. This means that Members may also lawfully share personal information amongst one another for these purposes outside the activities of the Forensics Standing Committee, e.g. in order to build a case of fraud/misconduct perpetrated by certain individuals. It is up to each Member to determine its own processes and controls the management of such sharing of information.

2.9. Members may accordingly also share personal information amongst one another (outside of the activities of the Forensic Standing Committee) for purposes of prevention and detection, e.g. sharing information for purposes of building a case of fraud or misconduct against a perpetrator. Members are free to determine their own processes and controls for the sharing of such information.

2.10. Another ground on which Members may be able to rely is the **obligation in law** basis referred to in paragraph 2.3.3. This is, in short, when a Member is obliged to process the personal information to comply with the law.

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

2.12. 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.

2.13. In order to protect against POPIA consequences here are some basic steps that Members can follow to ensure the continued sharing of personal information:

2.13.1. Establish the legitimate interest ground or grounds before sharing information;

2.13.2. Document your thinking – in the unlikely event of an ICO challenge, this will be vital;

2.13.3. Share information only where fraud concerns exist, documenting reasons where you do;

2.13.4. Update your data sharing request forms by specifying the relevant grounds for processing you rely on – this will provide the organisation you want information from with legitimate grounds to process the data lawfully and assist you with a fraud investigation.

Other conditions for lawful processing

2.14. Even where a lawful ground for processing exists, Members still have to comply with the other conditions of lawful processing as well, such as that only personal information that is necessary for the purposes of fulfilling the objectives Forensics Standing Committee may be shared and that data subjects must be informed that their personal information may be shared for purposes of the prevention of fraud and other misconduct.

2.15. Importantly, Members must have regard to the provisions of section 19 of POPIA, which provides that "*A responsible party 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 (1) loss of, damage to or unauthorised destruction of personal information; and (2) unlawful access to or processing of personal information*." When sharing personal information, Members accordingly have to ensure that the information is reasonably protected against unauthorised access.

3. COMPETITION LAW

3.1. The exchange of information between competitors, either directly or through a third party, such as ASISA, will attract competition scrutiny.

3.2. The Competition Commission has issued Guidelines on the Exchange of Competitively Sensitive Information between Competitors under the Competition Act No.89 of 1998 (as amended) ("**Guidelines**").

3.3. The Guidelines reiterate that industry bodies/trade associations generally facilitate the exchange of information between competitors and, as such, may be platforms for collusion.

3.4. However, the Guidelines only apply to "*competitively sensitive information*" as defined in the Guidelines, namely: "*information that is important to rivalry between competing firms and likely to have an appreciable impact on one or more of the parameters of competition (for example price, output, product quality, product variety or innovation). Competitively sensitive information could include prices, customer lists, production costs, quantities, turnovers, sales, capacities, qualities, marketing plans, risks, investments, technologies, research and development programmes and their results;*".

3.5. It is unlikely that any "*competitively sensitive information*" will be shared in the course of the work conducted by the Forensic Standing Committee, save for the statistics provided in terms of the **ASISA Policy on Statistics**, and more specifically the **Fraud and**

Forensics Annexure ("**Statistics Reporting**"). Information is exchanged for a legitimate purpose, is not aimed at impeding competition and the exchange brings about efficiencies for the Members and assists in consumer protection.

3.6. Insofar as any competitively sensitive information is shared for Statistics Reporting, measures have been implemented to ensure compliance with the Guideline:

3.6.1. **Age of the data**: In general, exchanging information that is a year old or older will not raise a concern; provided that no future conduct or current market information can in any way be inferred or deduced from the historic data. Sharing data for Statistics Reporting is an annual exercise (historical data

3.6.2. **Aggregation:** The exchanges of aggregated market data will not usually raise a concern, as it provides firms with only a picture of the overall market and does not enable firms to identify competitors or to monitor their actions or market positioning. Only aggregated information is shared in the Statistical Reporting exercise.

3.6.3. **Independent collator**: The information is received and collated by an independent third party who is subject to strict confidentiality undertakings.

3.6.4. **Availability of information**: Fraud and forensic statistics are made available to ASISA members, the public at large and stakeholders annually and simultaneously through publication thereof on the ASISA website.

3.7. There is no requirement under competition law that a Member must share information with all the other Members of the Forensic Standing Committee.

DOCUMENT HISTORY

Date	Publication/amendment
18 July 2024	First published

RESPONSIBLE SPA AND COMMITTEES

Responsible Board Committee	Technical and Operations Board Committee
Responsible Standing Committee	Forensic Standing Committee
Responsible Senior Policy Advisor	ASISA Point Person to the Technical and Operations Board Committee