# Protection of Personal Information Act: a new era of privacy for South Africa

Building a better working world

The past years have seen the world undergo a paradigm shift around privacy brought by the promulgation of the EU General Data Protection Regulation (GDPR), widely considered as one of the most disruptive laws of this past decade due to its stringent requirements and global reach. Data privacy can no longer be an afterthought due to associated compliance and reputational risks, and decision-makers are increasingly aware of the ethical and moral conundrum that a lack of transparency creates. In this environment, organizations are having to balance the competitive advantage brought by big data and artificial intelligence with their new responsibility toward their customers and partners.

Having recognized the need to regulate the use of personal information within the Republic of South Africa, the Parliament of the Republic of South Africa enacted the Protection of Personal Information Act (POPIA - Act 4 of 2013), with the bulk of sections[1] commencing on 1 July 2020, effectively ushering South Africa-based organizations into the new era of data privacy. Organizations have been granted a grace period of one year to normalize and implement the requirements of the law within their risk and compliance frameworks, and have to be able to demonstrate compliance by 1 July 2021.

Although POPIA exists since 2013, even pre-dating the GDPR, many organizations have been slow to react, and in many cases have underestimated the efforts required to implement a comprehensive privacy framework. Organizations subject to POPIA are bound by demanding requirements that require a re-thinking of the way processes and systems are designed, and in many cases the re-engineering of processes to absorb the new requirements imposed. This revamp to consider numerous privacy rights granted, privacy breach notifications and personal information impact assessments can be an onerous journey.

**For more cyber and privacy insights, visit:**

https://www.ey.com/en_gl/advisory/data-protection-privacy

[1] Sections 2 to 38; sections 55 to 109; section 111; and section 114 (1), (2) and (3). These sections highlight the responsibilities of organizations and effectively impose statutory requirements for the protection of personal information.

# What is POPIA?

POPIA is a data privacy law that complements section 14 of the Constitution of the Republic of South Africa, 1996, which provides that everyone has the right to privacy.

POPIA brings accountability on entities collecting, storing, analysing and managing personal information, while providing additional rights to individuals to maintain control of their personal information. POPIA applies to any organization that operates within the Republic of South Africa and to any organization which is not domiciled in South Africa but processes personal information in the country.

Unlike other privacy laws which apply only to personal information relating to living individuals, POPIA also applies to personal information relating to existing juristic persons, i.e. companies and other legal entities.

POPIA establishes the Information Regulator as the governing body for data privacy within the jurisdiction, empowering the body to monitor and enforce compliance to POPIA and the Promotion of Access to Information Act (PAIA - Act 2 of 2000).

POPIA prescribes a number of responsibilities and liabilities to entities that control and/or process personal information, and defines a number of new roles:

- **Responsible party:** a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information
- **Operator:** a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party
- **Data subject:** the individual or legal/juristic person to whom personal information relates
- **Personal information:** any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person

## Immediate next steps

Educate key stakeholders, including the board of directors

Assign responsibility for data privacy within the organization, in priority to the Information Officer and Deputy Information Officer(s)

Define data privacy policies and guidelines, considering your role as a responsible party and/or operator

Raise awareness of privacy principles within the organization, and provide specialized training to employees involved in the processing of personal information

Assess your current state of compliance, with a particular focus on governance, policies, technology, external dependencies (e.g. vendors), existing data flows (high-risk) and processing operations

Review and update agreements with your service providers to render them accountable to principles mandated by POPIA and ensure they support you in respecting your responsibilities

Assess privacy risks that exist throughout your processing activities, and perform personal information impact assessments to ensure adequate safeguards are implemented to mitigate such risks

# POPIA highlights

Applies to entities processing personal information within the Republic of South Africa

Fines up to R10 million or imprisonment term of up to ten years

Civil compensations and damages payable to affected data subjects as determined in court

Provides new rights to individuals , e.g. right to be notified, right to access of information, right to request correction, destruction or deletion of personal information, right to object to direct marketing, right to object to processing, right to object to automated processing, right to submit a complaint to the Information Regulator, and right to institute civil proceedings

Provides six conditions to lawfully process personal information namely consent, contractual obligations, legal obligations, legitimate interest of data subject, public authority tasks and legitimate interests of the responsible party or another person/company to whom the information is supplied

Responsible parties must maintain documentation of all processing operations and specific information must be disclosed in a PAIA manual, which is published on a platform that is easily accessible by data subjects and provided upon request

Personal information must be retained for defined periods of time as determined to be appropriate by the responsible party based on legal requirements, legitimate interests, contractual obligations, historical/statistical/research purposes or the explicit consent of the data subjects

# What are POPIA's principles and main requirements?

POPIA enhances the data privacy rights of data subjects whose personal information is processed within South Africa, either by a responsible party domiciled in South Africa or by a foreign company which uses South Africa-based operators. In order to enforce these rights and freedoms, POPIA brings the following principles around which all requirements revolve:

- **Accountability:** responsible parties can no longer avoid or transfer their accountability to privacy vis-à-vis data subjects and the Information Regulator. The onus to demonstrate compliance to the principles of the law throughout the processing lifecycle remains with the responsible party
- **Purpose specification:** organizations must have at least one lawful basis for processing, which includes consent, contractual obligations, legal obligations, legitimate interest of data subject, public authority tasks and legitimate interests of the responsible party or another person/company to whom the information is supplied
- **Processing limitation:** personal information must be processed in a manner which does not infringe on data subject's privacy, and which is relevant to the defined purpose.
- **Further processing limitation:** processing personal information for purposes other than for which the information was initially collected is only allowed if the new purpose is compatible with the initial purpose, consent has been provided by the data subject or the processing falls within very specific parameters provided by the law.
- **Information quality:** organizations now have the responsibility to ensure that the personal information they are processing is complete, accurate, not misleading and updated where necessary, and as long as this is reasonably practicable for the organization.
- **Openness:** transparency toward data subjects is a key requirement of POPIA. While the PAIA already imposed some documentation requirements on organizations, POPIA complements this by broadening the type of information to be provided to data subjects upon demand, and especially upon first collection of the information.
- **Security safeguards:** organizations must implement effective organizational and technical measures to safeguard personal information within their custody. POPIA advocates a risk- based approach, and any privacy initiative should be part and parcel of the organization's risk management and information security frameworks. POPIA also puts special emphasis on personal information, mandating disclosure to the Information Regulator and data subjects when these are affected.
- **Data subject participation:** POPIA brings additional rights to data subjects in an effort to maintain control over information that relates to them. Rights provided under the Act include:
  - Right to be notified about the personal information collected or if it has been accessed by an unauthorized person
  - Right to request access to this information
  - Right to request correction, destruction or deletion of personal information
  - Right to object to direct marketing
  - Right to object to processing, including where consent is obtained
  - Right related to objection to be subject to automated processing for profiling purposes, including performance at work, credit worthiness, reliability, location, health, personal preferences or conduct
  - Right to submit a complaint with the Information Regulator
  - Right to institute civil proceedings
- **Personal information impact assessment:** The Information Regulator published a regulation in December 2018 to complement the provisions of POPIA. The regulation adds the responsibility of the Information Officer to perform personal information impact assessments (PIIA) to ensure that adequate measures exist to comply with the conditions of lawful processing as per POPIA. While the regulation is not prescriptive on when PIIA should be performed, organizations need to obtain comfort that all processing activities affecting personal information are complying with POPIA requirements. PIIAs should be viewed as tools that can help organizations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIIA will allow the organization to identify and fix problems, reducing the associated costs and damage to reputation that might otherwise occur.

# Common pitfalls of implementing POPIA

Given POPIA dates back to 2013, many organizations are aware of its requirements and have a sound understanding of the principles of the law. However, there is the general impression of a relatively slow response across industries to implement these requirements, often driven by the lack of urgency given major sections of the law had not taken effect until 1 July 2020.

With a hard deadline of 1 July 2021, late adopters may now realize the demanding nature of implementing a fully compliant privacy framework. As they do, they should be careful about making some common mistakes:

- **Underestimating the level of effort:** often as a result of misunderstanding the breadth and applicability of POPIA, organizations have underestimated the level of effort required to implement the necessary process and technology changes to become compliant. The pervasive nature of POPIA means that it applies virtually to most departments/functions, and therefore requires action by a broad set of stakeholders within the organization, as well as by relevant third parties.
- **Inability to identify and understand the flow of personal information:** in practice, organizations with ineffective or low-maturity data governance frameworks may find it hard to identify all repositories of personal information (including of unstructured data), their owners and the flow of the information within and outside the organization. This is especially true for organizations that still heavily rely on paper-based processing.
- **Viewing it as a one-and-done exercise:** perhaps the most significant challenge is redesigning an organization's privacy and business processes to be able to demonstrate POPIA compliance on an ongoing basis, especially as the business, client base and product portfolio evolve. Getting to a position of POPIA-compliance is only the beginning as compliance is an ongoing responsibility. Building in sustainable approaches that provide the organization with the necessary flexibility to rethink how it designs, develops and delivers products and services to its customers is most critical.

# How should you implement POPIA?

Implementing POPIA should be viewed as an integrated exercise within the organization's risk governance framework. Data privacy touches on all aspects of an organization, reaching across people, processes and technology. A successful implementation program establishes a cross-functional team that supports the transformation of the organization, which is a critical step for a successful implementation. The data privacy framework should set the data privacy strategy within the context of the overall business and IT strategy, and focus on:

- **Program effectiveness:** there should be an enterprise view of the privacy program, allowing for organization-wide oversight, program-level reporting and escalation, and the application of consistent methodology throughout the lifecycle of the program.
- **Privacy risk management:** privacy risk needs to be well managed, in accordance with the overall risk management strategy. The privacy framework should link to the organization's risk and control framework and the third-party risk management framework. The various roles and responsibilities across the different lines of defense and functions (compliance, legal, privacy, cyber, etc.) should also be clearly defined.
- **Data management:** the program should embed the organization's data management and information security framework to manage the personal information throughout its processing lifecycle. The data architecture, classification and flows should enable the privacy strategy, while the information security framework should provide for appropriate data protection controls to secure the data at rest, during use and when being transferred outside of the organization's boundaries.
- **People and culture:** the talent requirements to properly implement the privacy framework need to be clear, and plans need to be defined to meet the organization's needs. Privacy also needs to be firmly embedded in the organization's culture, with ongoing awareness programs and training.

# Which parts of your organization will be most affected?

POPIA will have a significant impact across an organization's three lines of defense:

## 1 First line: business lines and technology

- **Business lines:** like other risks, the front-line businesses have to own the risks they create, including data privacy. They have to identify, measure, monitor and mitigate the risks associated with POPIA, implement the privacy principles, and design and maintain necessary and effective controls. They also have to implement enterprise-wide risk management frameworks developed by the second line, including in this context privacy risk, information technology risk, operational risk and overall enterprise risk management.

- **Operations:** those running day-to-day operations and supporting the front-liners have to develop and implement the necessary standards and procedures to secure personal information through the information life cycle. They should conduct personal information impact assessments to properly understand and manage the inherent risks. They also usually own relationships with vendors, and therefore play a big role in third-party risk management and in rendering third parties accountable to the organization's data protection and privacy policies and POPIA requirements and obligations.

- **Technology, security and data:** the technology group will have to consider what changes are required to the technology and data architecture to enable the proper handling, processing and security of personal information within the boundaries of the organization. This will include how the data is gathered (and through what channel), processed, stored, transferred (including cross-border and to other organizations) and, when necessary, destroyed. Tracking what data is affected will be a significant effort, especially as it relates to customer and account book-of-record, employee or contractor data (e.g., time and reporting systems), personal information used in customer relationship and marketing databases, and so on. The data management strategy that organizations may need to adopt to effectively execute against POPIA requirements — in terms of tagging, tracking, anonymising, encrypting — could be onerous, depending on how the organization determines it will address POPIA compliance. Those driving data analytics activities have to consider how they may be affected.

- **Innovation and marketing:** product development activities will need to embed privacy requirements as early as the design stage. organizations need to re-evaluate their product development strategies and determine how privacy considerations are built into the new products and services. Marketing materials will need to be revised to include the necessary disclosures, consents and notifications. Consent is one of the largest areas of challenge, especially around the need to consider whether you can 'grandfather' existing consent or whether you need to run a 'retrospective re-consent' exercise.

- **Procurement and contract management:** procurement and legal teams may need to evaluate existing standard contractual template terms to understand whether amendments are required to meet POPIA's requirements – for example around breach notification and increased obligations on operators. Organizations will need to identify which vendors are processing personal information and perform a risk-based prioritisation exercise to review existing contracts, identify required legal term changes, and potentially re-negotiate and 're-paper' existing contractual arrangements.

- **Human resources (HR), training and communication:** HR will need to consider if changes are required in regard to how employee or contractor information is segmented and managed, how HR information is reported upon and appropriate employee rights and consents are managed and adhered to. Working with the relevant functions and businesses, HR will need to re-evaluate the portfolio of awareness-raising, training and education activities and how those activities remain current and effective.

## 2 Second line: risk and compliance

- **Compliance:** the compliance function will have to validate that the privacy and information security strategies are aligned with each other and with legal requirements and regulatory reporting requirements.
- **Information risk management:** the information risk management function will need to review and revise information security policies, confirm that business-related procedures are in line with those revisions and assess if they are implemented effectively (either through reviewing first-line testing or conducting its own).
- **Privacy:** the privacy function has a critical role in managing the privacy framework with the support of other functional teams. The function will need to normalize all data privacy requirements applicable to the organization into privacy policies and procedures that will assist the organization in managing its privacy-related risks. The privacy function will also be responsible for guiding the organization in the implementation of privacy controls around key areas of business and compliance risks, such as privacy notices, breach management, requests relating to rights and management of operators.
- **Risk management:** the risk management function will need to work with the privacy, information risk management and information security functions to measure and monitor the evolution of data privacy and information-security related risks, and formalize tolerances for such risks according to the organization's risk appetite framework. This is particularly important for POPIA compliance given the potential for material fines and legal settlements or litigations. Organizations will need to re-evaluate privacy-risk reporting in this context.

## 3 Third line: internal audit

Internal audit will need to adapt its approach to consider privacy risks. Audit plans should cater for:

- Overall privacy framework validation against the requirements of POPIA
- Assessment of the effectiveness of cybersecurity risk management protocols
- Information security audits, especially around high value assets
- Reviews of processes to handle data subject requests and complaints
- Reviews of incident / breach management procedures
- Assessment of third-party risk management safeguards

In re-evaluating the scope of audits, internal auditors should assess and report on compliance to privacy and compliance key performance indicators to be defined by the first-line and second-line of defense. Some organizations may perform pre-implementation advisory audits, given the breadth of the requirements and expertise required to perform such assessments.

To support business stakeholder understanding of privacy, and the impact of POPIA on business lines and functions, EY professionals applied its privacy framework to POPIA and categorized 12 focus areas into 3 themes, as shown in Table 1.

**Table 1: POPIA requirements across the EY privacy risk management framework**

| | Focus area | Desired outcome |
|---|---|---|
| **Governance** | ▸ Accountability and compliance: privacy operating model, training/awareness, policy development | ▸ Creating structures and processes that help enable proactive, systematic and ongoing compliance reporting for senior management |
| | ▸ Privacy and security by design: privacy impact assessment, program design based on business model | ▸ Help achieving risk reduction and management through the application of requirements and tools integrated at various junctures in your process landscape |
| | ▸ Incident and breach management: data incident response plan and operational effectiveness process | ▸ Help enabling rapid management of a data breach, including internal investigations and external reporting |
| | ▸ Privacy data assessment: data use case management/framework, data classification, data flow mapping, data discovery, cloud discovery, high-value asset identification | ▸ Help establishing and operationalizing governance over personal data usage and analytics as well as understanding the most meaningful attributes of your data that impact compliance risk and optimized use |
| **Use of data** | ▸ Consent and privacy notification: freely given and explicit consent, right to withdraw consent, privacy notices | ▸ Increasing transparency through explicit consent to process data and privacy notifications |
| | ▸ Data protection: identify and access management, technology selection, encryption strategy | ▸ Approach designed to achieve data protection and enhance your security hygiene |
| | ▸ Data rights management: data subject's right to access, correction, erasure and/ or objection | ▸ Supporting your organization to support data rights to access, deletion, portability and rectification |
| | ▸ Records management: attach requirements to physical files, electronic documents and emails | ▸ Strategy and program design that balances global privacy regulation with data protection, legal and business needs |
| **Validation** | ▸ Contract management: assessment of service-level agreements, assess internal or third-party contracts to identify gaps or identify opportunities to strengthen language | ▸ Discovery and revision of contractual provisions pertaining to privacy and security, including data permissions and restrictions |
| | ▸ Third-party risk management: third-party risk assessment, compliance monitoring and data controls | ▸ Understanding, designing and monitoring for the management of your third-party personal data access, protection, responsibilities and liabilities |
| | ▸ Internal and external assurance: internal audit assessment, third-party attestation, certification against industry standard | ▸ Providing independent confirmation that governance, risk management and internal controls as they relate to both privacy and security are designed and operating effectively |
| | ▸ Continuous monitoring and improvement: compliance monitoring program design, monitoring of key controls, dashboard reporting for management | ▸ Designing for ongoing awareness of privacy and security compliance to facilitate risk management and support optimisation of the control environment |

# The clock is ticking: act quickly

In enacting POPIA, the Information Regulator provided organizations one year to achieve compliance.

Now, with limited time remaining, many organizations still have a long way to go to make all of the necessary changes to be ready for 1 July 2021. Building an approach that is sustainable beyond that date is even more challenging. Time is of the essence.

The first step is assessing gaps that need to be addressed; here, a risk-based (not just legalistic) assessment is strongly suggested.

It is important that the right governance and program structure is put in place from the outset. A cross-functional team is required. To be successful and sustainable, this effort cannot be buried in legal and compliance.

A thorough POPIA gap assessment is needed, one that reaches across the swath of affected businesses and functions. To the extent that the assessment is too narrow, it will make timely implementation much harder. Important factors will be identified too late, causing decisions made to degrade the quality of the approach, leave the organization open to regulatory scrutiny and ultimately cost more as work needs to be redone to make the approach sustainable on an ongoing basis.

And, finally, there is a need to prioritize. After all, the timeline to implementation is getting shorter, so organizations need to prioritize those activities that get to baseline compliance. Building more sustainable processes can be completed after July 2021, as necessary.

It is time to act.

# How EY teams can help

EY people understand the challenges that POPIA brings and have assisted clients across industries in assessing their current privacy framework and in implementing privacy programs in compliance with requirements of various privacy laws, including the GDPR and POPIA.

The Data Protection and Privacy service offerings cover all the domains that will assist in defining a comprehensive privacy framework and improve the privacy culture within your organization.

| Offering | Description |
|---|---|
| **Data Protection and Privacy Assessment, Strategy and Transformation** | Services to measure, design and improve the overall Data Protection and Privacy Strategy Program and its Governance |
| **Data Governance and Data Ethics** | Services to measure, design and improve the Data Governance Program. Support of Data Ethics strategy |
| **High Value Asset (HVA) Protection** | Services to design and implement HVA protection programs, including identifying, classifying, governing and securing high value information |
| **Data Protection and Privacy Technology Enablement** | Services to assist clients in the selection and implementation of technology solutions for data protection and privacy |
| **Managed Services** | Services to assist clients with ongoing operational execution of data protection and privacy processes |
| **Data Protection and Privacy Awareness and Training** | Provisions of services in the area of Awareness and Training, including workshops and gamification |

# EY contacts

**Tony De Bos**

Partner, EY Advisory Netherlands LLP
EY Global Data Protection and Privacy Leader

+31 6 29084182
*tony.de.bos@nl.ey.com*

**Andy Ng**

Partner, Cybersecurity
EMEIA Advisory Data Protection and Privacy Leader

+44 7525 238 593
*andy.ng@uk.ey.com*

**Shameem Goolamun**

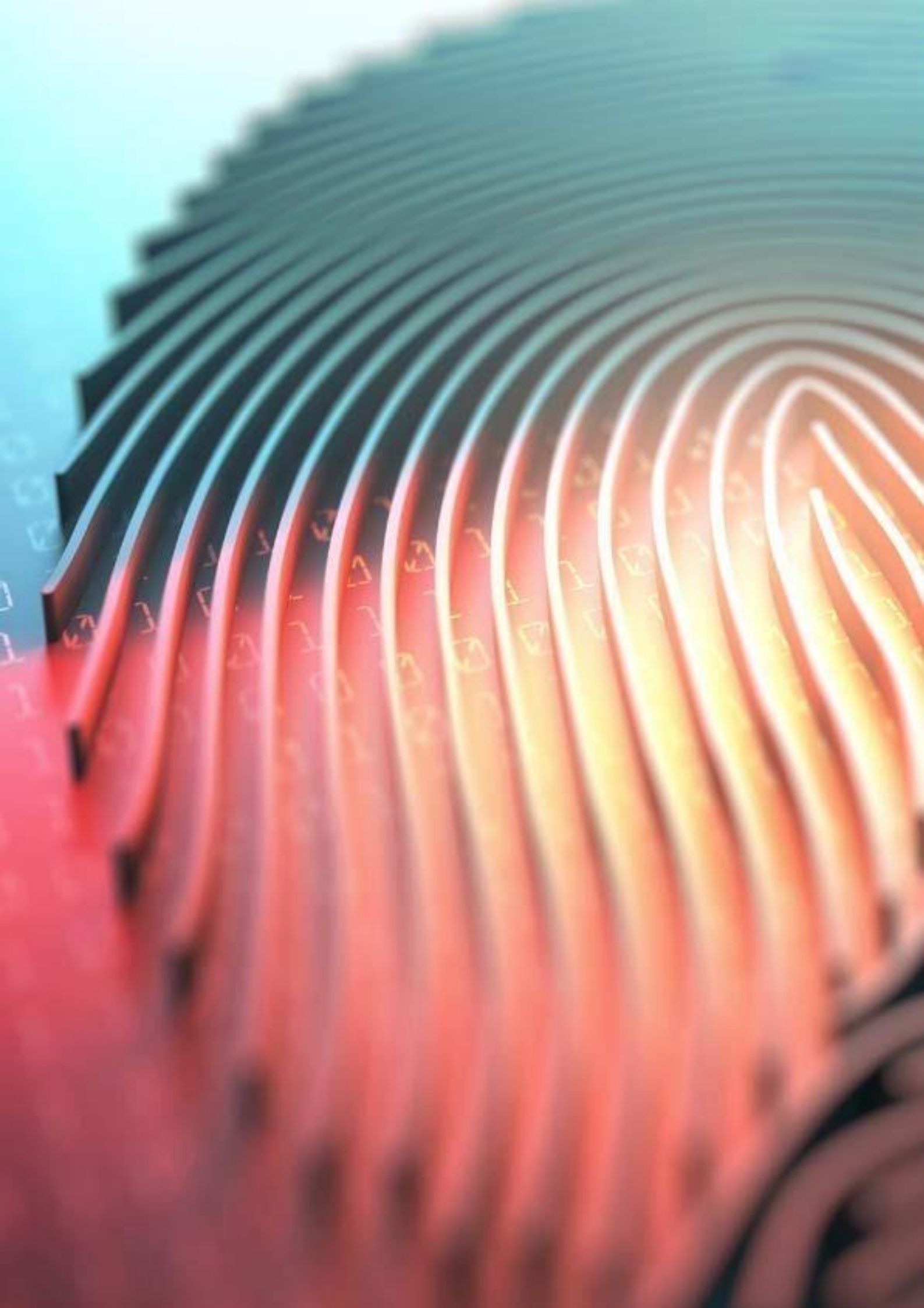
Associate Director, Ernst & Young Ltd
EY Africa Data Protection and Privacy Leader

+230 5774 9072
*shameem.goolamun@mu.ey.com*

**Cathy Gibson**

Partner, Ernst & Young Advisory Services (Pty) Ltd
EY South Africa Cybersecurity Leader

+27 82 330 7711
*cathy.a.gibson@za.ey.com*



## EY | Assurance | Tax | Transactions | Advisory

### About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.



EYG no. 007421-20Gbl



ey.com