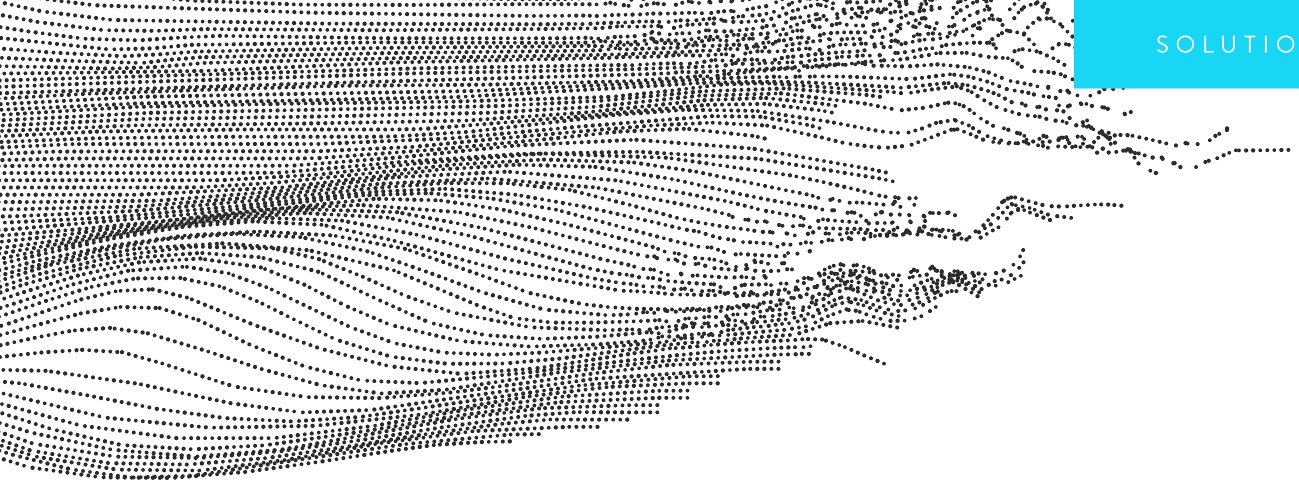


SOLUTION BRIEF

Delphix for POPIA Compliance

Eliminate Compliance Risk in Lower Environments

South Africa has ushered in a new set of data privacy requirements to protect citizens from misuse and exposure of their personal data. The Protection of Personal Information Act (POPIA) was initially passed in 2013 and came into effect on July 1, 2020, but will not be enforced until July 1, 2021, giving businesses a little time to prepare.

POPIA focuses on ensuring that organisations responsibly protect and govern sensitive personal information, while giving consumers greater control over how their data is collected, processed, and shared.

POPIA provides a set of eight conditions businesses must satisfy when processing personal information:

- Accountability for all the personal information in your control.
- Lawfulness, providing legally justifiable reason for collecting personal information.
- Purpose specification and not storing it for longer than necessary to meet that purpose.
- Further processing limitation for only the reason you originally collected it.
- Information quality, accuracy, and completeness.
- Openness, providing consumers with information on how and why you process their personal information.
- Security safeguards, taking reasonable steps to secure the personal information in your control, and reporting any data breaches as soon as reasonably possible.
- Data subject participation, allowing data subjects to access their personal information and correct or erase any inaccurate personal information.

POPIA imposes fines, penalties, and possible prison time for privacy violations and holds businesses responsible for implementing “reasonable security procedures” to protect personal information from unauthorised disclosure.

Who Must Comply?

POPIA, like GDPR and CCPA, mandates that businesses protect personal information when collecting, storing, moving, or sharing data. Every type of company, regardless of size, sector, or location, must comply with POPIA if:

- Based in South Africa
- Based outside of South Africa, but processes personal information within South Africa

What Data is Protected?

POPIA defines "personal information" as:

"Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person"

POPIA protects personally identifiable consumer, employee, or (even in some cases) company information. Within this definition a "natural person" means an individual and an "existing juristic person" refers to a corporation or charity.

Examples of personal information protected by POPIA include not only names, addresses, phone numbers, and ID numbers, but also beliefs, religion, medical history, and more.

What is not considered personal information?

In the POPIA Section 6, several exclusions to what is defined as personal data are outlined. The first exclusion declares that personal information, which has been irreversibly de-identified, is not regulated by POPIA and therefore the exposure of de-identified information does not constitute a violation.

POPIA SECTION 6 EXCLUSIONS

1. *(1) This Act does not apply to the processing of personal information—*

    i. *in the course of a purely personal or household activity;*

    ii. *that has been de-identified to the extent that it cannot be re-identified again;*

Compliance with POPIA

Achieving compliance with all eight conditions of POPIA is a multifaceted undertaking that requires organisation-wide collaboration to address policies, technologies, and human practices associated with the management of personal data.

While no single technology will satisfy the entirely of the requirements that POPIA drives, the Delphix Data Platform can play a pivotal role in helping businesses:

- Identify and assess the data environments impacted by POPIA and easily determine degree of risk.
- Create an actionable inventory of sensitive data.
- Define and implement policy to secure personal data subject to POPIA, and control who has access to what data, when, and where.
- Report and audit the actions taken to achieve compliance with key provisions of the regulation.
- Irreversibly de-identify personal information in non-production environments, such as dev/text, analytics, and AI/ML modeling.

To comply with POPIA, business must take reasonable action to ensure that personal information will not be exposed if a systems breach occurs. The only way to ensure this will not happen is to not have personally identifiable data contained in systems and processes. Data that is irreversibly de-identified is not considered personal data. Delphix Compliance meets the definition of irreversibly de-identifying personal information.

Delphix Eliminates Data Risk in Non-Production Environments

Delphix provides a programmable data infrastructure that automatically delivers secured, virtualised data into dev/test, analytics, AI/ML, and cloud environments whether on-premises, hybrid, or multi-cloud. Delphix APIs can automate a comprehensive range of requirements, including data refresh, cleanup, integration, time machine, version control, and most importantly, sensitive data discovery, data masking and compliance. The Delphix cloud-native management interface provides a central point of control and a global view of enterprise data.

Delphix synchronises with any production data source, virtualises the data it collects, then provisions virtual data copies to developers, testers, analysts, or data scientists. Data copies from Delphix are highly space-efficient, readable/writable, and can be controlled (e.g. refreshed, bookmarked, branched) via APIs and through a simple-to-use, self-service interface. Most importantly, terabytes of data can be provisioned in minutes.

With the ability to provision, de-provision, mask, and otherwise control data across all non-production environments, the Delphix Data Platform can become the single point of control for defining, enforcing, and auditing data privacy policies for POPIA.

01

Contain up to 80% of a company's sensitive data

02

Data is often copied over and over

03

Many more people have access

04

Less focus on protecting against breaches

05

Often reside on unprotected devices such as laptops

Non-production environments for development, testing, analytics, ML/AI, and reporting represent as much as 80% of the attack surface for data breaches and are often less scrutinised from a security perspective.

How Delphix Addresses Key POPIA Provisions

Since development, testing, reporting, and analytics data stores contain up to 90% of an enterprise's personal data, non-production environments can represent the single largest source of POPIA risk. Masking this data neutralises the risk of breach for these environments.

Delphix provides programmable profiling of sensitive data and algorithm-based masking to irreversibly replace sensitive data with fictitious yet realistic values while retaining referential integrity across dev/test, analytics, and data science environments.

- Automated identification of personal data values.
- Irreversible masking that ensures data cannot be restored to its original, sensitive data
- Realistic data that does not compromise dev/test, analytics, or AI/ML models
- Referential integrity for masked data across sources and clouds.
- Out-of-the-box and customisable algorithms that require no specialised programming expertise.

Data Profiling: Identify and Assess POPIA Risks

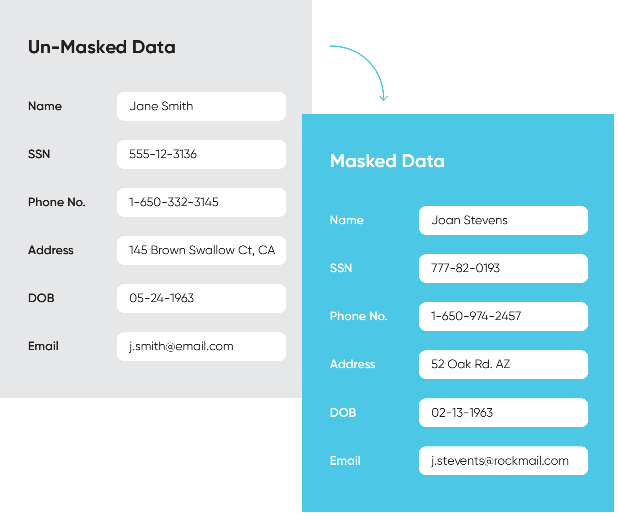
Identifying where personal information resides is a necessary precursor to meeting several POPIA requirements. Delphix profiles data sources and automatically pinpoints personal information such as names, email addresses, and social security numbers to help businesses:

- Locate environments in scope for POPIA, then determine how much and where personal data resides within those environments.
- Execute a targeted approach for protective measures through data masking.
- Monitor data environments on an ongoing basis for continuous compliance.

Delphix comes pre-configured to locate the data values and fields designated as “personal” under POPIA. This provides businesses an enterprise-wide view of POPIA risk. It also helps compliance teams map out which environments contain what types of data, positioning them to more easily respond to consumer requests to expunge data or report on how data is being processed or shared.

Data Masking: Irreversibly De-Identify Personal Information

Once Delphix identifies personal information in data sources, it determines recommended de- identification algorithms, then masks the personal data. Delphix masking algorithms produce realistic but irreversible values with referential integrity across disparate sources. Delphix is simple enough to allow business users to create enterprise-level masking policies for POPIA that define what data should be masked, where, and how. Users can then consistently deploy those policies across different data sources and locations, such as a public cloud, on-premises, or a hybrid environment.



Un-Masked Data

Name	Jane Smith
SSN	555-12-3136
Phone No.	1-650-332-3145
Address	145 Brown Swallow Ct, CA
DOB	05-24-1963
Email	j.smith@email.com

Masked Data

Name	Joan Stevens
SSN	777-82-0193
Phone No.	1-650-974-2457
Address	52 Oak Rd. AZ
DOB	02-13-1963
Email	j.stevents@rockmail.com

Once data is profiled and an inventory of masking algorithms applied, Delphix ensures that sensitive data is continuously identified and continuously protected. Delphix profiling can automatically be run on a periodic basis, discovering changes to the data structure and automatically refreshing the rulesets. Masking algorithms can be applied to the new sensitive data, ensuring that enterprises continuously protect their customer and employee data in compliance with POPIA.

Data Governance: Define and Implement Compliance Policies

Beyond the application of masking as a security measure, Delphix serves as the control plane for managing non-production data across the complete data lifecycle. Delphix automatically provisions masked and unmasked data copies with the ability to associate permissions with copies to determine how they are accessed and manipulated. Administrators can also use Delphix to de-provision or inactivate data copies at the click of a button. It can do this for multiple, heterogeneous data sources across on-premises, cloud, and hybrid environments. Collectively, these capabilities allow businesses to understand and control:

- Where data environments containing POPIA-relevant personal information reside.
- Which datasets are moved across and within different locations or clouds.
- Who is allowed to see unmasked data versus who can access only masked data.
- How long data environments are deployed and active.
- A robust API set also allows teams to embed these capabilities into compliance workflows or integrate Delphix with other security solutions to provide comprehensive protection against data loss.
- Ensure only masked data is replicated to non-production / cloud environments using Selective Data Distribution (SDD), a throttled, encrypted and incremental data replication feature.

Since development, testing, reporting, and analytics data stores contain up to 90% of an enterprise's personal data, non- production environments can represent the single largest source of POPIA risk.

Report And Audit Data Privacy Actions

Delphix logs all security and administrative actions to give businesses robust reporting and auditing capabilities. In particular, Delphix maintains an inventory of data masking policies that document how specific types of personal data were discovered and secured, then tracks exactly where and when those policies were deployed. Distribution of all masked and unmasked data is also captured, creating a continuous record of data governance measures across time and space.

In the event of a POPIA audit, businesses can easily report against the state of their non-production environments, including the security policies in place as of a specific point in time. Delphix even allows businesses to report against the state of their production environments. Since Delphix stays synchronised with production data sources as they change over time, it can provision historical point-in-time copies that recreate a data environment reflective of a specific moment—down to the second or even transaction—to enable detailed forensics or auditing with respect to POPIA.

BELKIN PROTECTS CUSTOMER AND GOVERNMENT DATA IN COMPLIANCE WITH GDPR, CCPA, AND OTHER REGULATIONS

Masking ensures that sensitive customer and government data is obfuscated when building and sharing reports, helping Belkin stay in compliance with all data privacy regulations. Automating the task of finding sensitive information vastly reduces the time it previously took to manually identify and remove the data. Using algorithms to mask data, Belkin is then assured the sensitive information is protected in all environments and reports.

In addition, by masking sensitive information in their development and testing environments, Belkin accelerated data refreshes for development environments from once a year daily, thus increasing frequency and accuracy of ERP system updates. This enables Belkin to release customer facing solutions, which rely on the backend ERP, faster and dramatically enhance the customer experience.

"Delphix does two things great—masking and data virtualisation. Delphix masking helps us protect customer and government data in compliance with GDPR, CCPA, and other regulations. Delphix virtualisation helps us go faster with on demand data environments for application development."

LANCE RALLS, Global CIO

PAYBAY GUARANTEES PROTECTION OF PERSONAL DATA AND ENSURES COMPLIANCE WITH GDPR REQUIREMENTS

PayBay is a leading mobile payment and digital services provider, specialising in the development of state-of-the-art electronic money, mobile and analytics platforms. PayBay runs over 40 mission-critical applications including payment processing, card management, contract management and couponing platforms. All of these applications require development and testing environments, but PayBay needed an automated way to eliminate sensitive data from these environments to keep customer information secure while continuing to enhance the customer experience.

As part of a transformation project around risk and compliance, PayBay is leveraging data masking to guarantee the protection of personal data, thus ensuring compliance with GDPR requirements. The impact will go far beyond security. Automating the anonymisation of data and integrating data security makes data delivery much faster enabling agile development and testing. PayBay is also using data masking to accelerate real-time analytics, application streaming, machine learning for fraud detection, and the migration of core applications to the cloud.

"Delphix not only reduces our risk of failure, but accelerates our business and empowers our organisation to make better decisions. Our goal is to be a digital business, run by data driven services. Delphix gets us there faster."

ANTONIO DE DONATO, Head of Digital Enterprise Architectures

DELTA DENTAL KEEPS MEMBER DATA SECURE AND IRREVERSIBLY ANONYMISED IN CLOUD ENVIRONMENTS

As the largest dental benefits system in the U.S., Delta Dental depends heavily on software applications to support the orchestration of core business processes such as contracts management, customer on-boarding, and claims processing. Moving to the cloud is part of Delta Dental's long-term digital strategy to improve scalability and time to market across its application portfolio. However, to protect cloud data from breach and enable regulatory compliance, Delta

Automated masking non-disruptively collects data from Delta Dental's production applications and applies masking to that data to protect any confidential information. With fresh, secure data available in the cloud, Delta Dental can easily deliver new virtual data copies to a team of over 200 developers, in just minutes and accelerate development of innovative applications.

> *"The combination of Delphix and AWS gives us the agility we need to succeed in today's application-driven economy. By easily and securely moving data to the cloud, we're able to release new features to the market faster, while also lowering cost and risk."*
>
> **SHAN SWAMINATHAN,** VP of Application Delivery and DevOps

ABOUT DELPHIX

Delphix is the industry leader in programmable data infrastructure. Delphix automates the biggest constraint in digital transformation programs—the data. With our multi-cloud data platform, enterprises modernize legacy apps 20% faster, migrate to the cloud 30% faster, and release software 50% faster, while maintaining compliance with GDPR, CCPA, HIPAA, and other data privacy regulations.

| delphix.com | info@delphix.com | +1.650.494.1645
Q321-00027