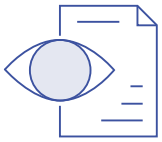
ACHIEVE SINGAPORE PDPA COMPLIANCE

The Singapore Personal Data Protection Act of 2012 (PDPA) was established to protect the nation's citizens from privacy breaches, making it illegal for organizations to store copies of Singaporean consumers' National Registration Identity Cards (NRIC). While the act itself is highly localized, it has international ramifications for any entities operating or doing business in the Republic.

Any organization that fails to comply with the PDPA may suffer fines of up to $1 million. Avoid these penalties and maintain compliance with Enterprise Recon solutions from Ground Labs.

Identify and secure PII on an ongoing basis to maintain Singapore PDPA compliance Ground Labs' Enterprise Recon empowers companies to identify and remediate NRIC data across their entire network, including PII located on workstations, servers, database systems, emails or cloud storage platforms.

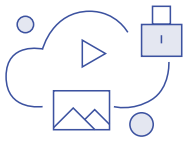
HOW GROUND LABS CAN HELP ENSURE PDPA COMPLIANCE



Identify over 300 different types of data and file formats, including data stored in servers, on desktops, email, and databases, on prem and in the cloud.

Support PDPA compliance obligations under the Protection Obligation with custom reporting and analytics available in the Enterprise Recon dashboard.

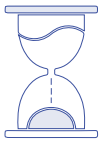
Discover data that is stored on legacy or older systems that are prohibited by the PDPA.



Search within both structured and unstructured data sources including files, databases, emails, cloud, big data and more.

Low resource requirements that allow mission-critical system use.

Reduce the overall time and investment required to reach and uphold PDPA compliance, even as regulations change over time.



Reduce the time required to map, analyze and remediate data before being transferred overseas into cloud storage, in accordance with the PDPA Transfer Limitation Obligation.

Execute a proactive approach to data security - as opposed to a reactive approach that relies on damage control post-breach - to build a stronger foundation of trust within your organization.

Book a complimentary sample data analysis with Ground Labs at https://go.groundlabs.com/book-a-demo

GROUND LABS

TAKING STEPS TOWARDS PDPA COMPLIANCE

As of 1 September 2019, Singaporeans are no longer able to use their National Registration Identity Card (NRIC) number for uses such as signing up for retail membership or redeeming free parking in a mall. This change was the result of the updated Singapore Personal Data Protection Act (PDPA) NRIC Advisory Guidelines, which has tightened the rules surrounding the use, collection and disclosure of Singapore NRIC numbers.

To comply, organizations have modified their systems so that NRIC numbers are no longer required as primary identifier.

Ground Labs has identified a ticking time bomb in the form of legacy data stored from previously non-compliant data capture processes. Despite there being no new data captured, existing data, stored for 10 or more years in past-dated folders on file servers, archives, backups and old emails, is often ignored.

Where is all the existing NRIC data hiding?

Desktops or laptops

Regardless of personal data's is supposed to be stored, files end up stored locally for auto-recovery, cache or performance reasons, which makes desktops a ripe target for attack.

File servers

File servers allow multiple departments to access shared information, such as a registration forms that contains names, NRICs, mailing addresses and phone numbers. Often there is no accountability or process to identify and securely discard of such information, which can result in 10, 15 or even 20+ years of data remaining on the file servers and their associated archives.

Email

Emails are generally percieved as secure, thus used for sending sensitive information. This leads to transmission of personal data, including Singapore NRIC information. However, once the data has served its purpose it is rarely deleted.

Customer Relationship Management (CRM) systems

One common area where data security violations occur in CRM systems is the use of free text comments and notes fields, often used to store information such as NRIC, passport, driver's license or even credit card numbers. When multiple employees have access to this information, and with the majority of CRM systems being cloud-based, the security of such personal information cannot be easily assured.

Application databases

Organizations use application databases for storing customer details or handling payment-related information. Having data stored across so many different platforms may cause organizations to inadvertently overlook securing certain locations, leaving them vulnerable to exploitation.

Cloud storage

As cloud storage providers often offer unlimited storage, there is no urgency to free up storage space, resulting in sensitive data remaining hidden in the cloud long after the data is obsolete.

Big data platforms

Big data platforms such as Teradata and Hadoop allow companies to systematically analyze and process complex and voluminous data sets. However, most organizations do not fully consider data sensitivity, which can result in large volumes of Singapore personal data finding its way into big data sets.

Archive and backup systems

Archives typically contain data that is no longer active but necessary for retention, while a data backup is a complete copy of your organization's data for disaster recovery purposes. This essentially means that data archives and backups contain duplications of sensitive data, and must be afforded the same level of security and protection.

To be PDPA-compliant, you must know where all Singapore personal data resides

At Ground Labs, we understand that data security should be a "business-as-usual" activity. Our flagship product Enterprise Recon makes data discovery simple. The best way to create awareness is to run a proof-of-concept (POC) for your organization on a sample dataset which can yield real results in a short amount of time. To understand how straightforward it can be to mitigate compliance risks, check out the Enterprise Recon solution, or book a free demo at a time that suits you.