InfoConnect

Data Masking

Safeguard Your Sensitive Data with Data Masking

Data Masking allows protection of sensitive information, such as PII and financial records, from unauthorized access. By replacing actual data with fictitious yet realistic values, data masking allows businesses to use datasets safely for testing, analytics, or data sharing without compromising privacy. Data masking ensures compliance with regulatory standards and maintains data integrity, allowing organizations to balance between data security and utility.

Personally Identifiable Information (PII) includes:

- Full names
- Social Security Numbers
- Bank account details
- Addresses, phone numbers

last_name	first_name	ssn	gender	state
Smith	Bob	123-45-6789	M	CA
Doe	Jane	098-76-5432	F	PA
King	Stephen	888-67-5309	M	WI
Savage	Randal;	135-24-6789	M	FL
Downer	Debbie	918-55-4680	F	NC

→

last_name	first_name	ssn	gender	state
Smith	Bob	xxx-xx-xxxx	M	CA
Doe	Jane	xxx-xx-xxxx	F	PA
King	Stephen	xxx-xx-xxxx	M	WI
Savage	Randy	xxx-xx-xxxx	M	FL
Downer	Debbie	xxx-xx-xxxx	F	NC

Diagram: example of data masking: replacing social insurance numbers with 'x.'

MYR 1.0mil
Potential fine for PDPA non-compliance

120 mil
Personal data records leaked in Malaysia

$4.45mil
Global average cost per breach incident

Data Breaches Mitigated by Data Masking

Internal / Insider Threats

Accidental or malicious exposure of sensitive data by employees.

Data in Testing Environments

Non-production databases often contain sensitive production data but lack equally robust security.

Stolen or Lost Devices

Exposure of unencrypted sensitive information through lost devices.

Common Applications of Data Masking:

- Software development and testing (in non-production environments)
- Data analytics
- Third-party data sharing
- Cloud migration and data sharing
- Compliance with privacy regulations (e.g. PDPA, PDP Law)