DPEX

DATA PROTECTION EXCELLENCE NETWORK

Managing Data Protection in the New Normal

Benjamin Shepherdson
CIPM, GRCP, EXIN(GDPR, INFOSEC)
Country Manager/Director
Straits Interactive Sdn Bhd

About Straits Interactive

Straits Interactive enables
"Trusted businesses & Responsible marketing."

We help organisations achieve **systematic Data Privacy & GRC** (Governance, Risk Management & Compliance) so as to build trust with customers…

Through:
- **People** (Training, Certification)
- **Process** (Advisory, Audit & Policy Automation Services)
- **Systems** (Integrated GRC & Data Privacy)

Our Offices

Data Privacy – DATA PROTECTION LAWS

European Union
Up to 4% of global annual turnover for companies
Euro 10m-20m

Singapore
Up to S$1 million.
$10k per DNC breach
Legal Proceedings

Malaysia
RM 500,000
Up to 3 years jail

Taiwan
Up of five years jail in addition to or instead of fines of up NT$500k- 1m (sensitive data)

Australia
Up to A$1.7 million for each breach

Hong Kong
Fines - HK$500k – 1m and 3 to 5 years jail

Philippines
1-3 years jail unauthorized disclosure (up to Php 1m fine)
3 to 6 years jail – sensitive data breach (up to Php 4m fine)

India
fine of up to INR 500,000 or up to 3 years jail or both

New Laws

Indonesia

Thailand

India

New Data Protection Laws or amendments in the region

India
DP Bill
(end 2020)

China
Draft Law
(end 2020)

Philippines
DPA
(2012)

Thailand
PDPA
(2020 May)
(Enforcement postponed 2021)

Indonesia
PDP Bill
(end 2020*)

Singapore
PDPA
(2010)

Malaysia
PDPA
(2010)

Countries with Comprehensive Laws covering the public sector

Upcoming amendments

Data Privacy Operational Compliance

2 Important Life Cycles

The Information Lifecycle

CUDS

Compliance Framework

APSR

Key Questions - Management Questions …That need to be answered

What are the risks?

What is required under data protection laws?

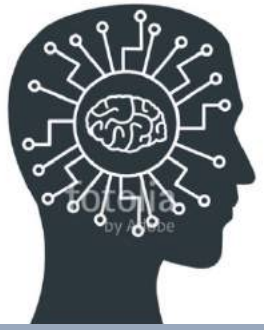
Who needs to get involved?

How do we go about complying?

What are the Risks?

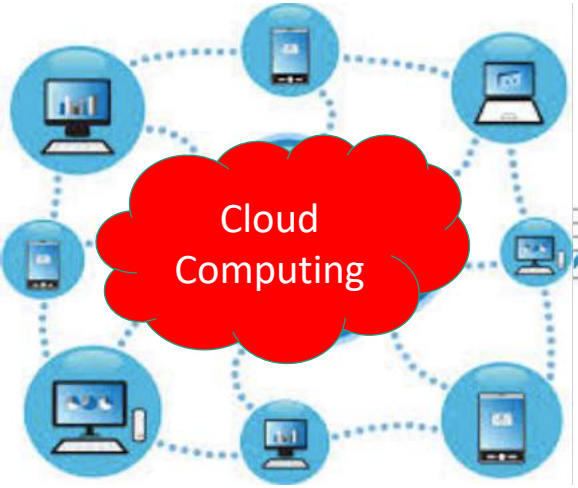
Privacy Invasive Technologies

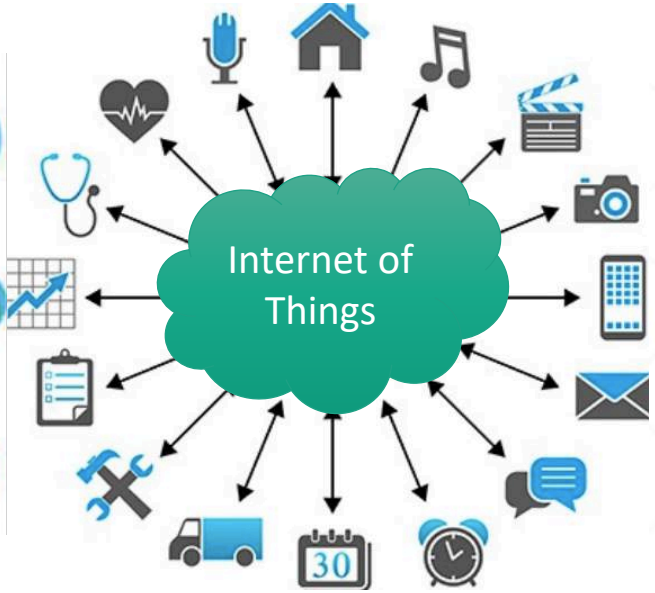
Social Media



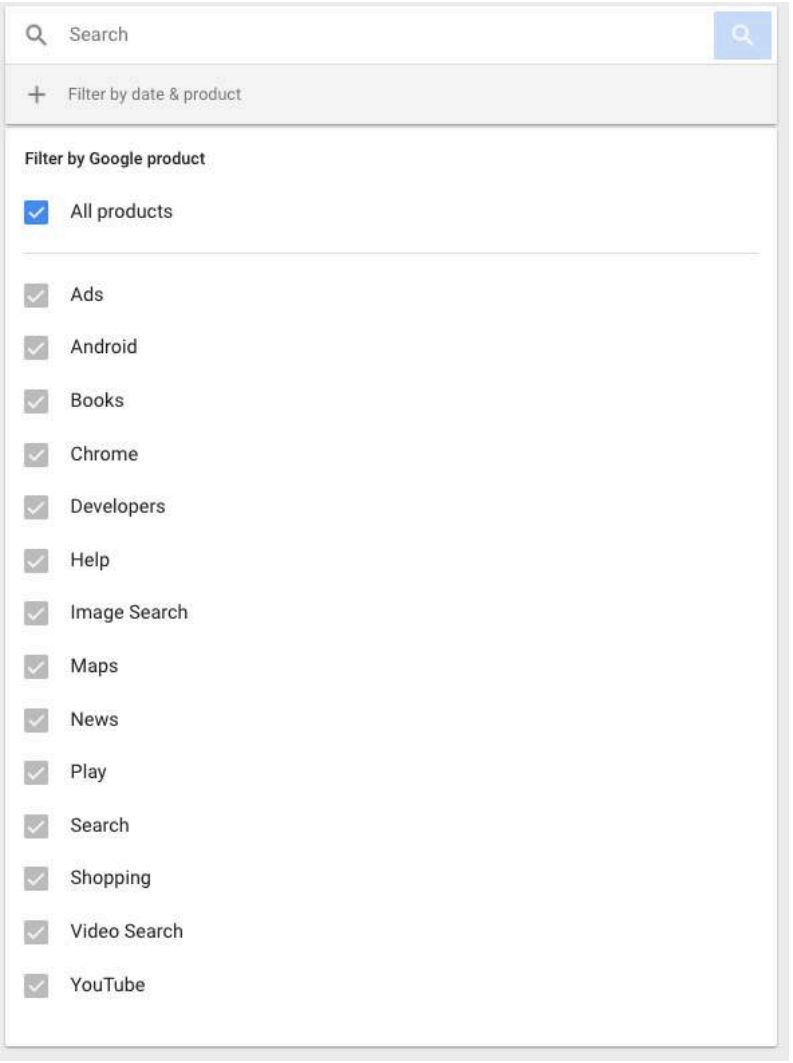
Artificial Intelligence

Block Chain





Implications of a Connected World



What Google Knows

Google compiles enough data to build comprehensive portfolios of most users—who they are, where they go and what they do—and the information is all available at google.com/dashboard. Here are just a few things WSJ reporter Tom Gara found out about himself.

GMAIL
134,966
All of Tom's emails since he first got a Gmail account in 2004. Google also stores his 6,147 chats.

CONTACTS
2,702
Google knows the people that Tom emails the most. At the top is a friend in Egypt.

GOOGLE SEARCH
64,019
Google thinks Tom performs most of his searches around 8 a.m. ET, but this is probably skewed by years spent outside the U.S.

YOUTUBE
9,220
Videos Tom has watched, listed in chronological order, including a series viewed in June about canoes.

TOM GARA

ANDROID DEVICES
3
Google knows all of Tom's synched Android phones, including the old Nexus S phone that he gave to his mom.

GOOGLE PLAY
117
That's how many apps Tom has downloaded from Google's store.

WALLET
3
Credit cards (two expired) saved in Google Wallet, plus two shipping addresses and 13 itemized purchases since June 2009.

PASSWORDS
35
Number of website passwords saved in Google's Chrome browser.

DOCS
855
Documents Tom has created, plus the 115 he has opened that belong to other people.

LOCATION
Willunga, South Australia
Due to an unknown glitch, Google bases Tom's location from one of his old Android phones, which he gave to his mother in Australia.

Graphic by Alberto Cervantes/The Wall Street Journal

http://www.zerohedge.com/news/2013-08-01/what-google-knows-about-you

What is Required Under the PDPA?

Rules

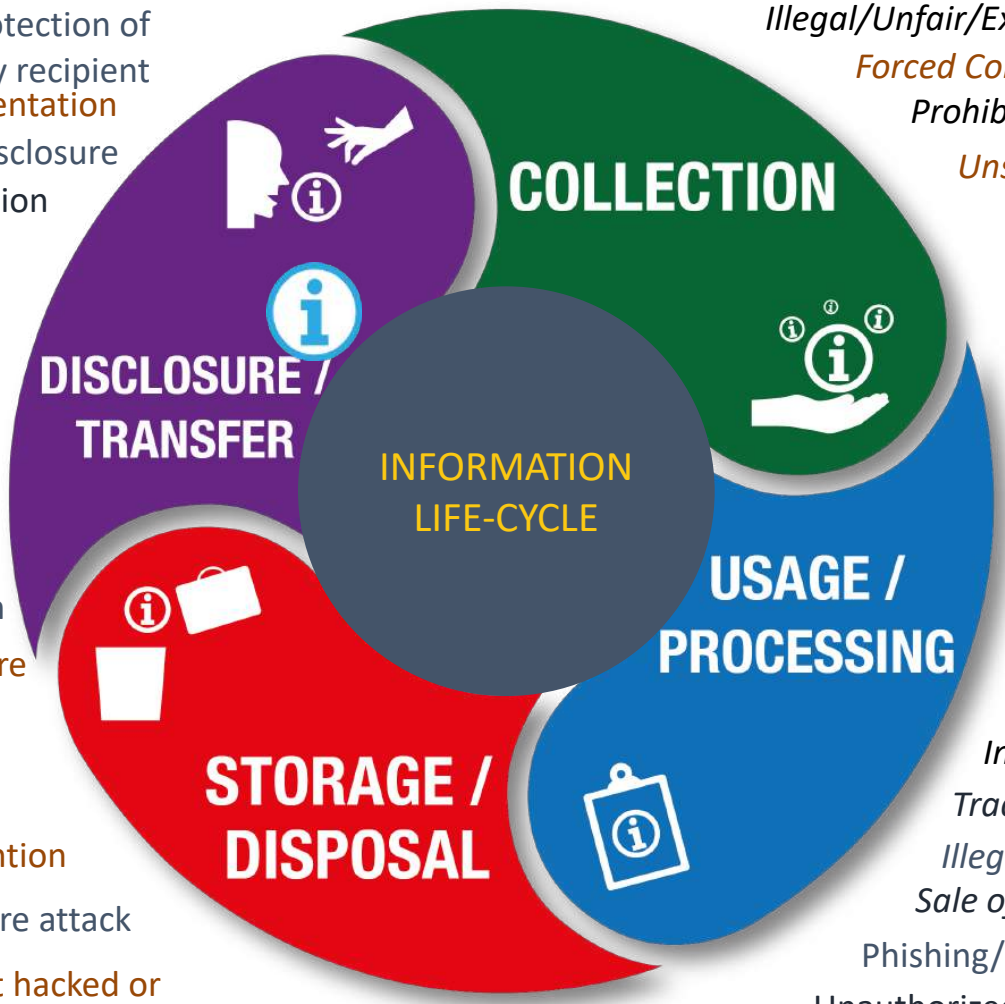
Rules

Rules

Rules

Information Life-Cycle

What are the risks relating to personal info?



Violation of cross-border rules

Inadequate care and protection of personal data by recipient

Misrepresentation

Leakage or accidental disclosure

Insecure Transmission

Unauthorised disclosure to third parties

Denying individual from exercising rights

Denial of correction to personal data

Denial of access to personal data

Indiscreet Conversation

Excessive/Illegal disclosure

No Consent given

Illegal/Unfair/Excessive Collection

Forced Consent/No choice

Prohibit Withdrawal of consent

Unsecured collection

Misleading purpose

No notification of purposes

Purpose not clearly specified

Unauthorized secondary purpose

Inaccurate/outdated data

Contacting individuals who are blacklisted/opt-out or in DNC Registry

Error in processing

Negligent Usage / Misuse

Invasion of privacy/ analytics

Tracking of usage / surveillance

Illegal / inappropriate use

Sale of Data

Phishing/Social Engineering

Unauthorized access to information

Confidentiality breached

Improper disposal

Unlimited retention

Virus/Malware attack

Data/Account hacked or compromised

Unprotected device

Lost or misplaced archives / device

Identity Theft

Unsecured data

Information Life-Cycle – 40 Exposures

What is required under the Data Protection Laws?

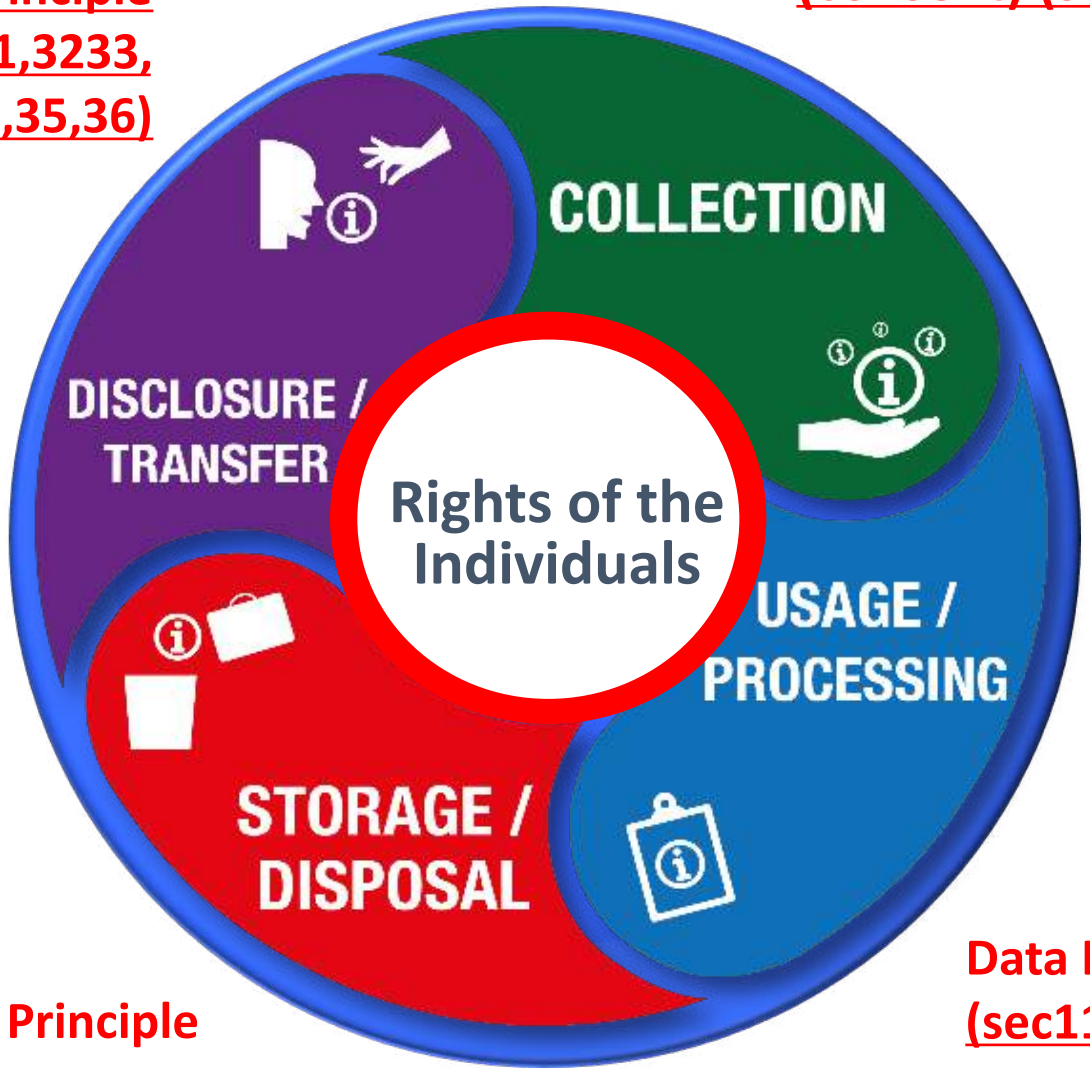
Malaysia Personal Data Protection Act 2010

What is Required Under the PDPA?

General Principle (consent) (sec6(1))

Access Principle (sec12,30,31,3233, 34,35,36)

Notice & Choice Principle (sec7)



Disclosure Principle (sec8)

General Principle (Lawful Processing / Non Excessive Processing) (sec6(2))

Retention Principle (sec10)

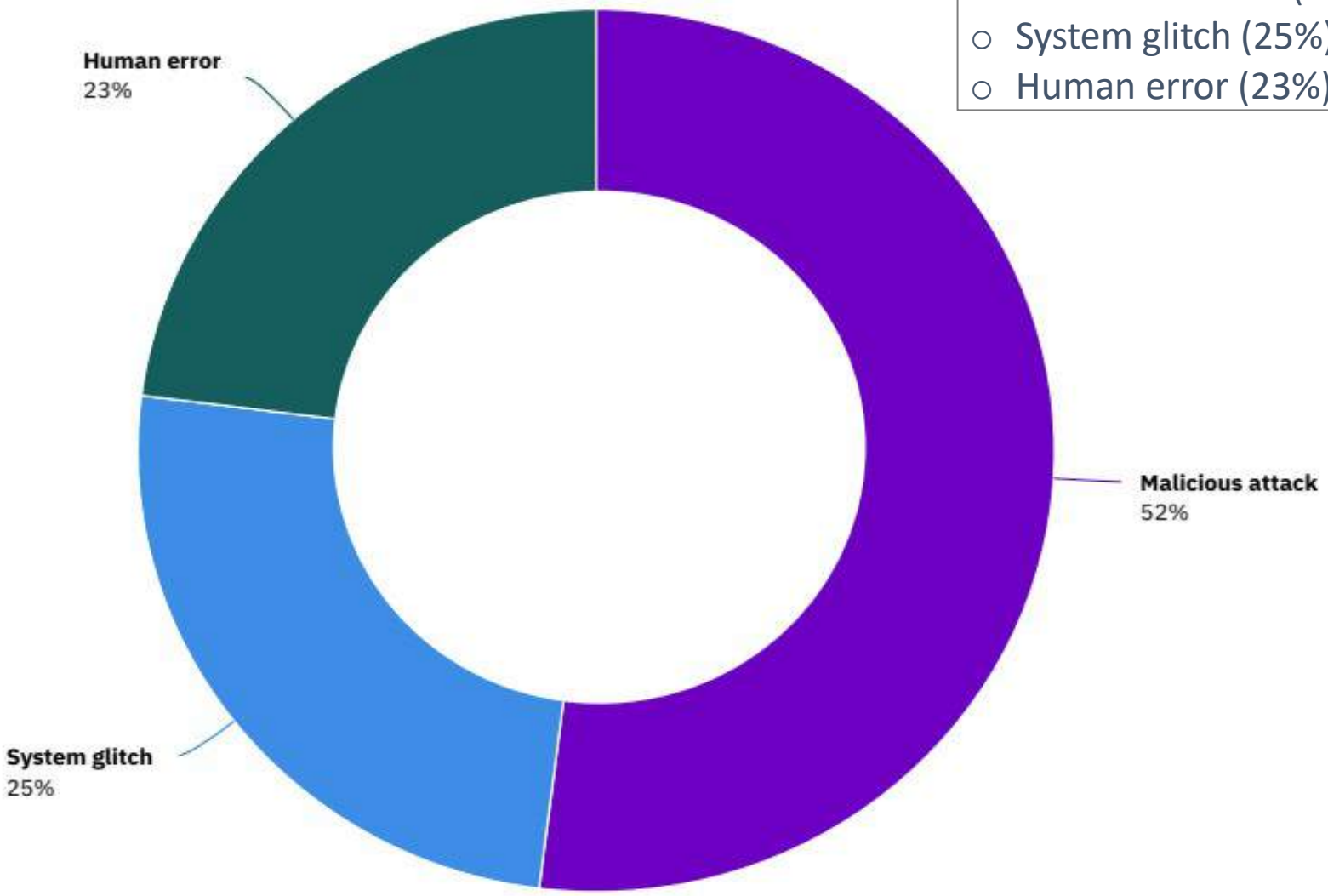
Data Integrity Principle (sec11)

Security Principle (sec9)

Data breach root cause breakdown in three categories

Root causes:

- Malicious attack (52%)
- System glitch (25%)
- Human error (23%)



2020 Cost of a Data Breach Report - Ponemon Institute

Impact of a Data Breach

Besides fine:

- **Financial losses**
  - Average of >US$140 per compromised record for recovery (Source: Ponemon Institute, 2016 Cost of Data breach report)
- **Loss of customers & business**
- **Trust & Confidence**
- **Stock price**
- **Potential litigation**
- **Brand name impacted**

Singapore

PDPC fines IHiS, SingHealth combined S$1 million for data breach following cyberattack

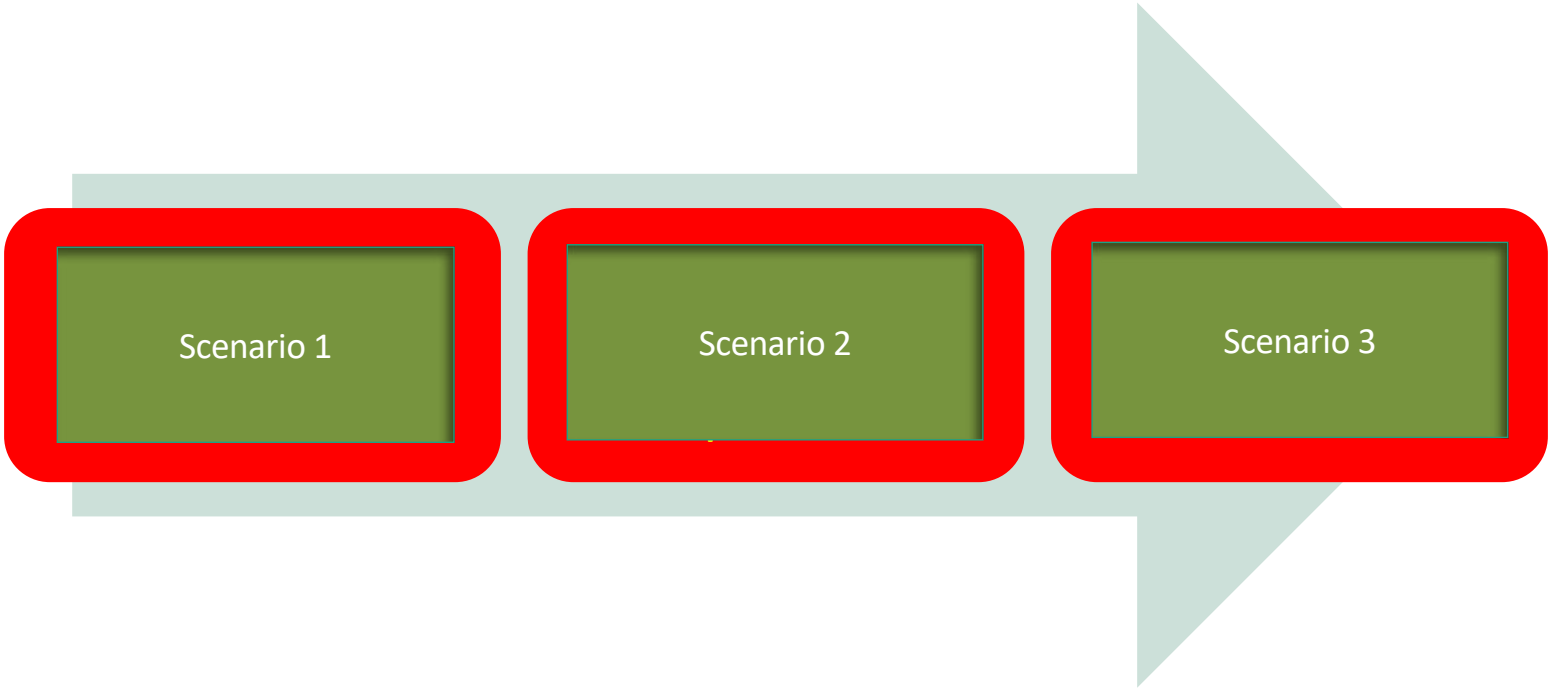
SINGAPORE: The Personal Data Protection Commission (PDPC) has slapped a fine of S$750,000 on IHiS and S$250,000 on SingHealth for breaching their data protection obligations under the Personal Data Protection Act (PDPA), it said in a statement on Tuesday (Jan 15).

Data Breach case could have been prevented if the organisation had:

✓ IDENTIFIED RISKS

✓ CONTROLS and MEASURES to align with Corporate Objectives in their Data Privacy Risk Management exercise

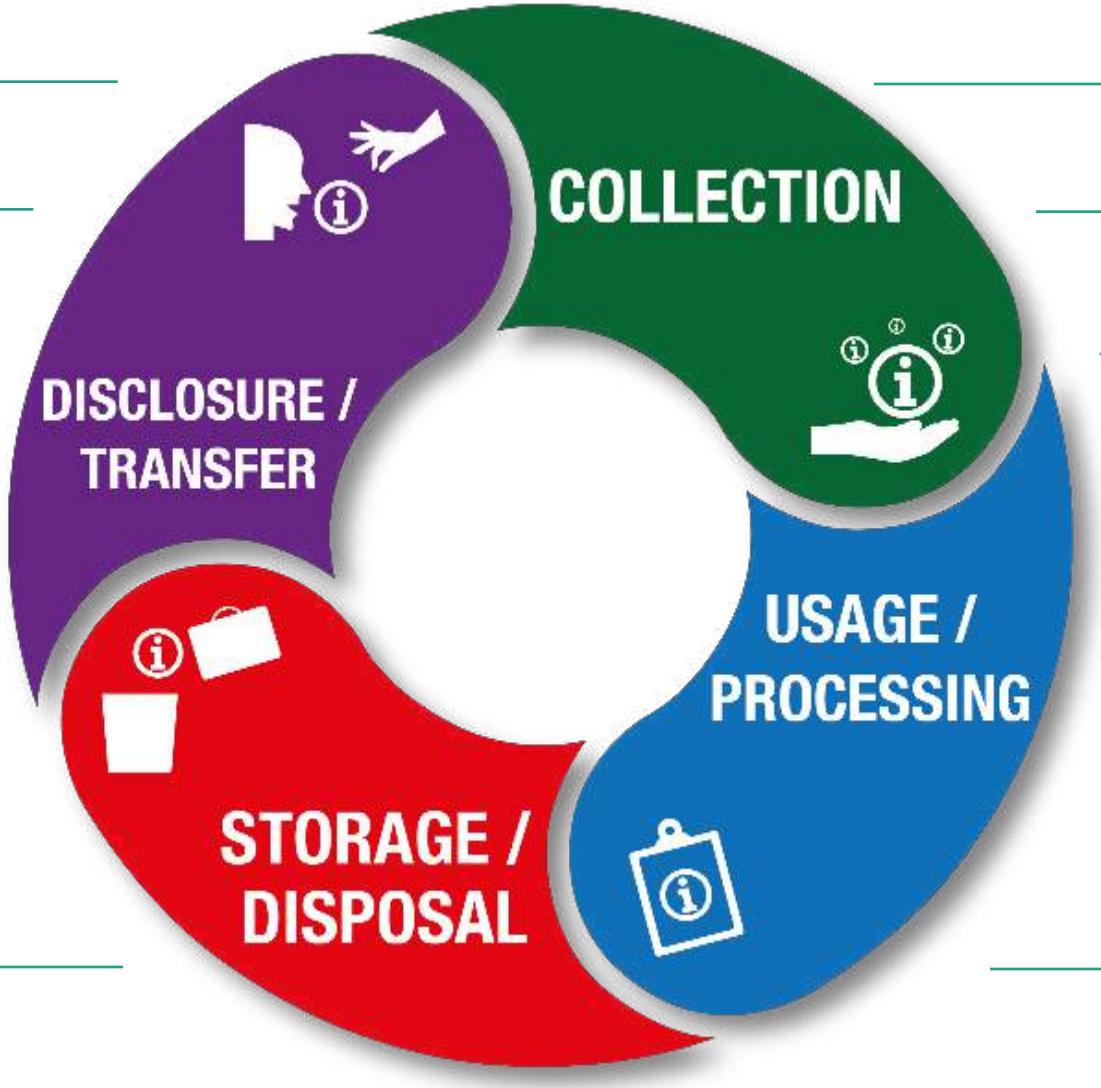
Why Data & Privacy Breaches Happen



Who needs to get involved?

Who Needs to get involved?

Involve departments that process personal data



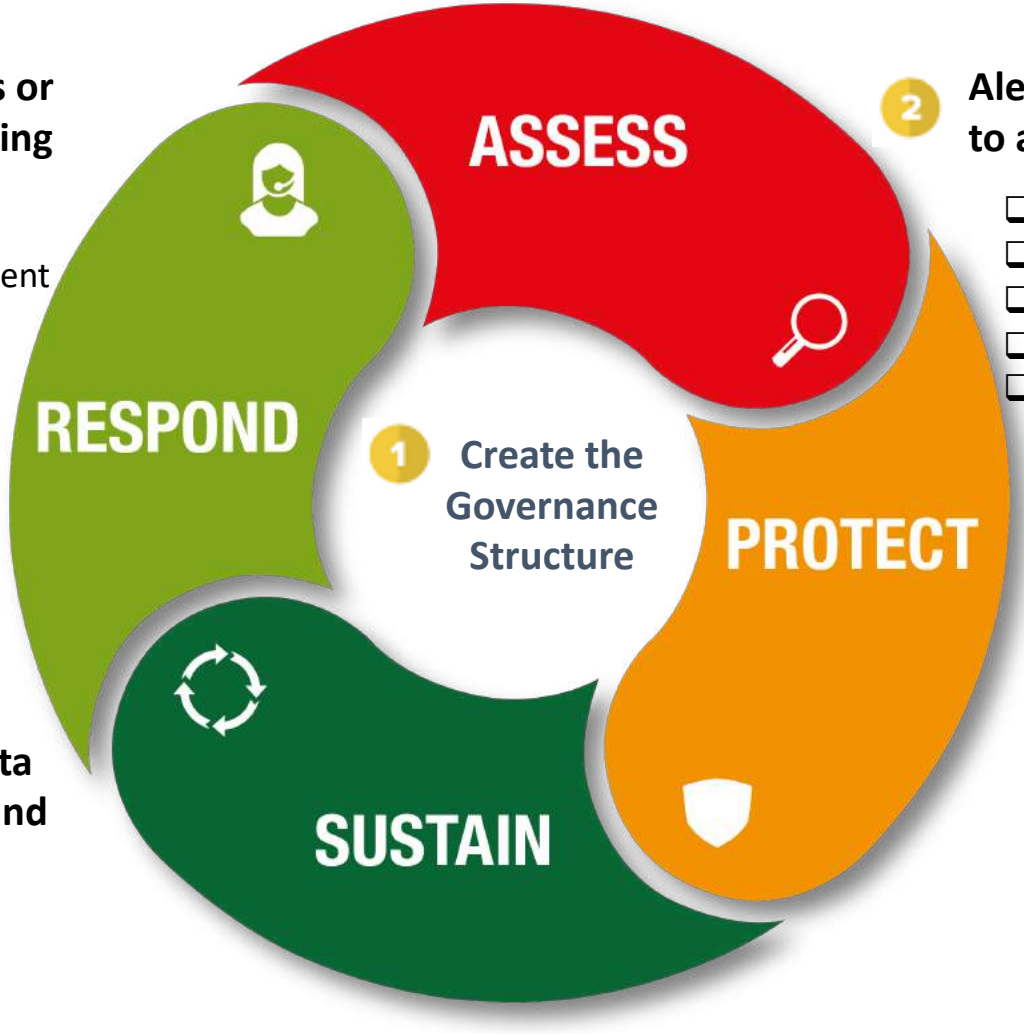
Information Life Cycle

How do we go about complying

SUMMARY : 5 Steps to Comply
Operational Compliance

5 Handling queries or complaints; Liaising with the JPDP

- ❑ Response management
- ❑ Accountability
- ❑ Preventing harm



2 Alerting your organisation to any risks

- ❑ Data Protection Assessment
- ❑ Personal Data Inventory Map
- ❑ Personal Data Flow (CUDs)
- ❑ Baseline On-site Audit
- ❑ DPIA

4 Communicating the internal personal data protection policies and processes

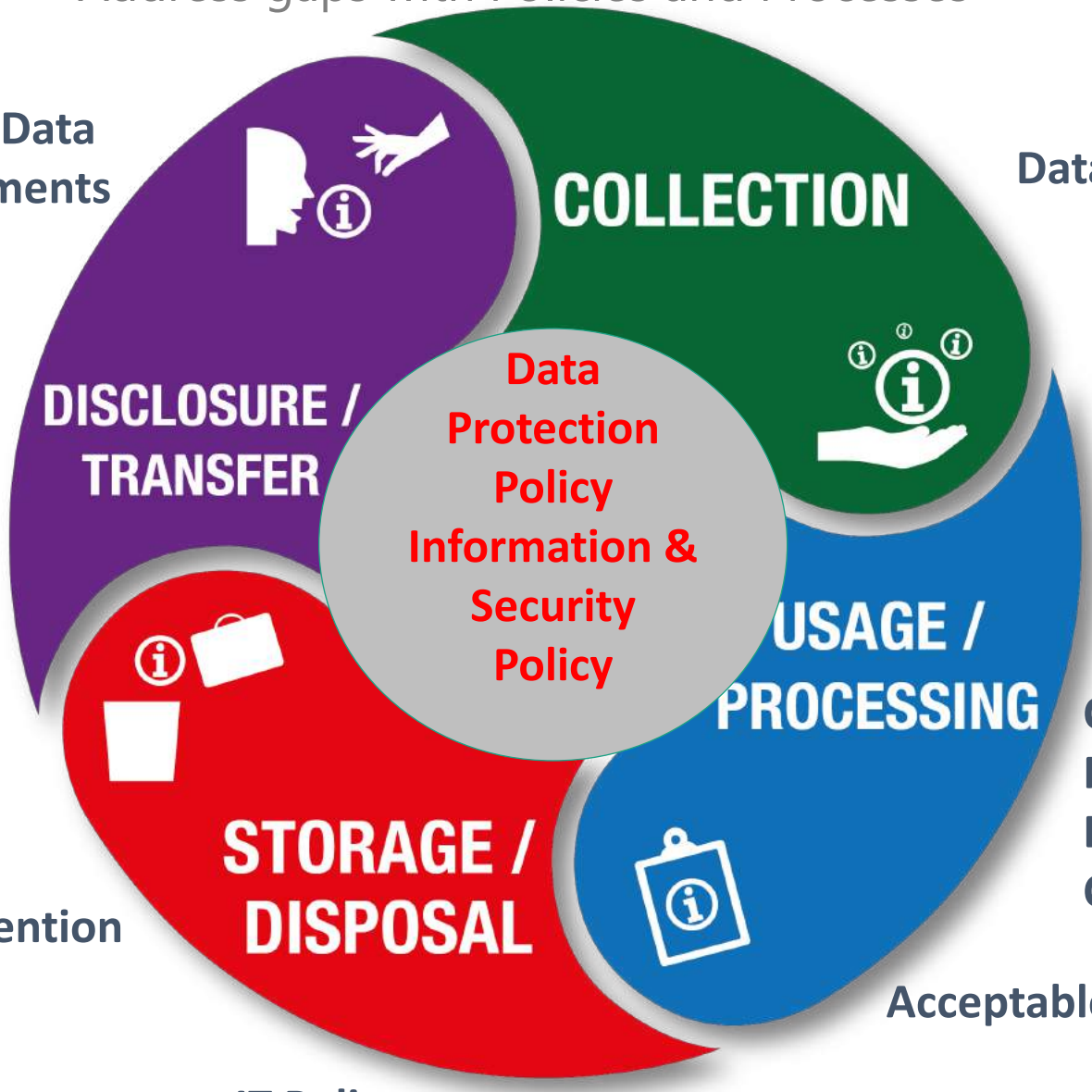
- ❑ Monitoring
- ❑ Auditing
- ❑ Communications

3 Developing good policies for handling personal data

- ❑ Address risks (AART)
- ❑ Information Security
- ❑ Info-sec policy
- ❑ Controls (TAP)
- ❑ **Data Protection Policy**

How to Comply?

Address gaps with Policies and Processes



3rd Party Outsourcing / Data sharing agreements

Privacy & Data Protection Notice

Consent Clauses in Contracts/Forms

Confidentiality/ PDPA in Employment Contracts

Acceptable Use Policy

Bring your Own Device Policy

IT Policy

Document Retention Policy

Non Disclosure Agreement

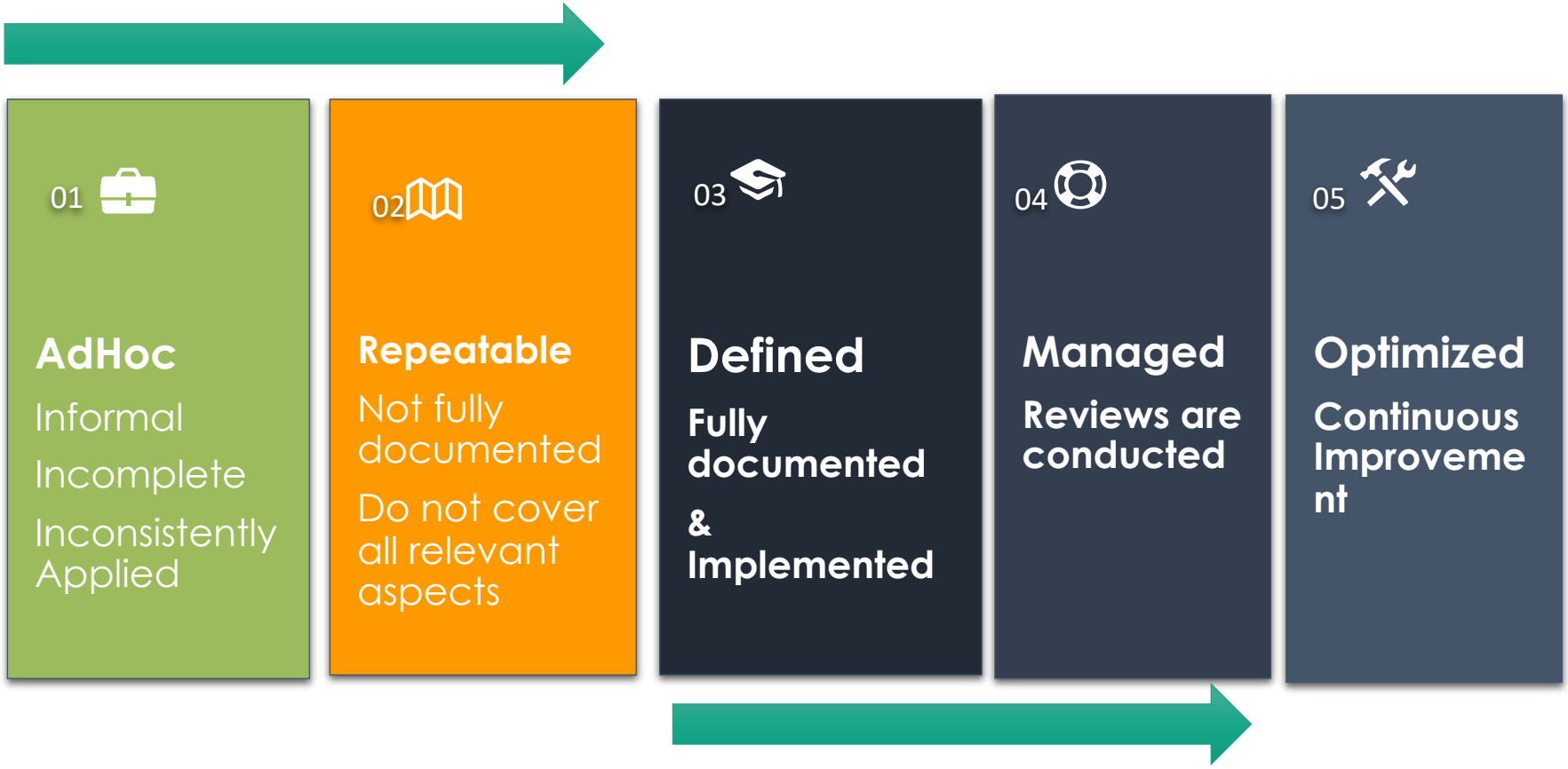
7 Mistakes Most Organisations Make

- Insufficient data protection measures
- Little or no information security practices
- Vulnerable IT infrastructure to online threats
- Improper training – policies not communicated
- Disjointed practice
- Complacency
- Trusting third parties & poor contracts

Privacy Maturity Model (AICPA/CICA)

Where is your organization in?

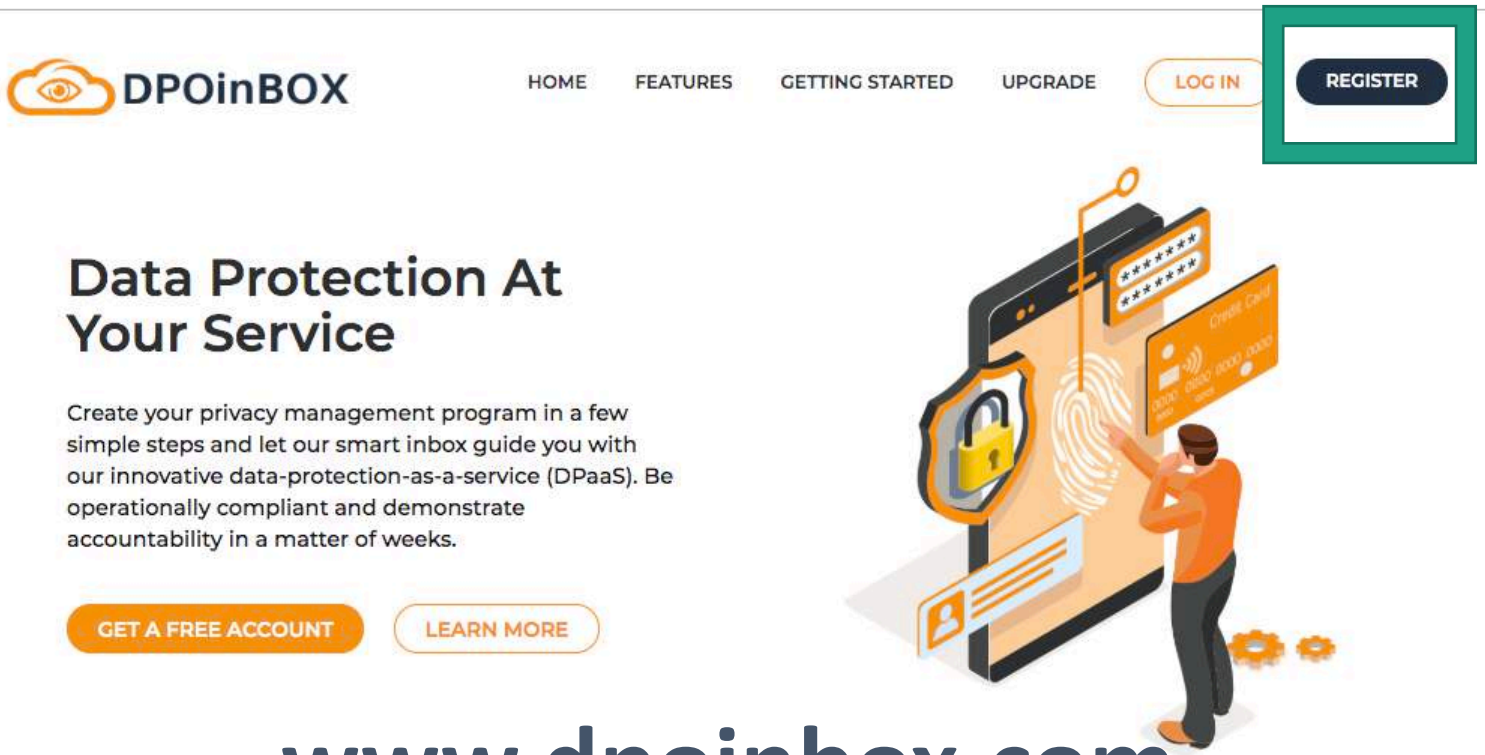
"OPERATIONALIZED"



Giveaways!!!

Data Protection Officer InBox (DPOinBOX)

Data Protection Solution



www.dpoinbox.com

DPOinBox

Registration page

DPOinBOX

Achieve operational compliance with data protection laws.

Implement data protection or privacy management programme.

Demonstrate accountability to regulators.

For optimal experience, it is recommended that you use Chrome, Safari or Firefox

DPOinBOX powered by GeneXist

Register to start your free account

Please complete all fields so that we can tailor the experience to your needs.

First Name

Last Name

Email

Contact No

Registered Company Name

Malaysia

Industry

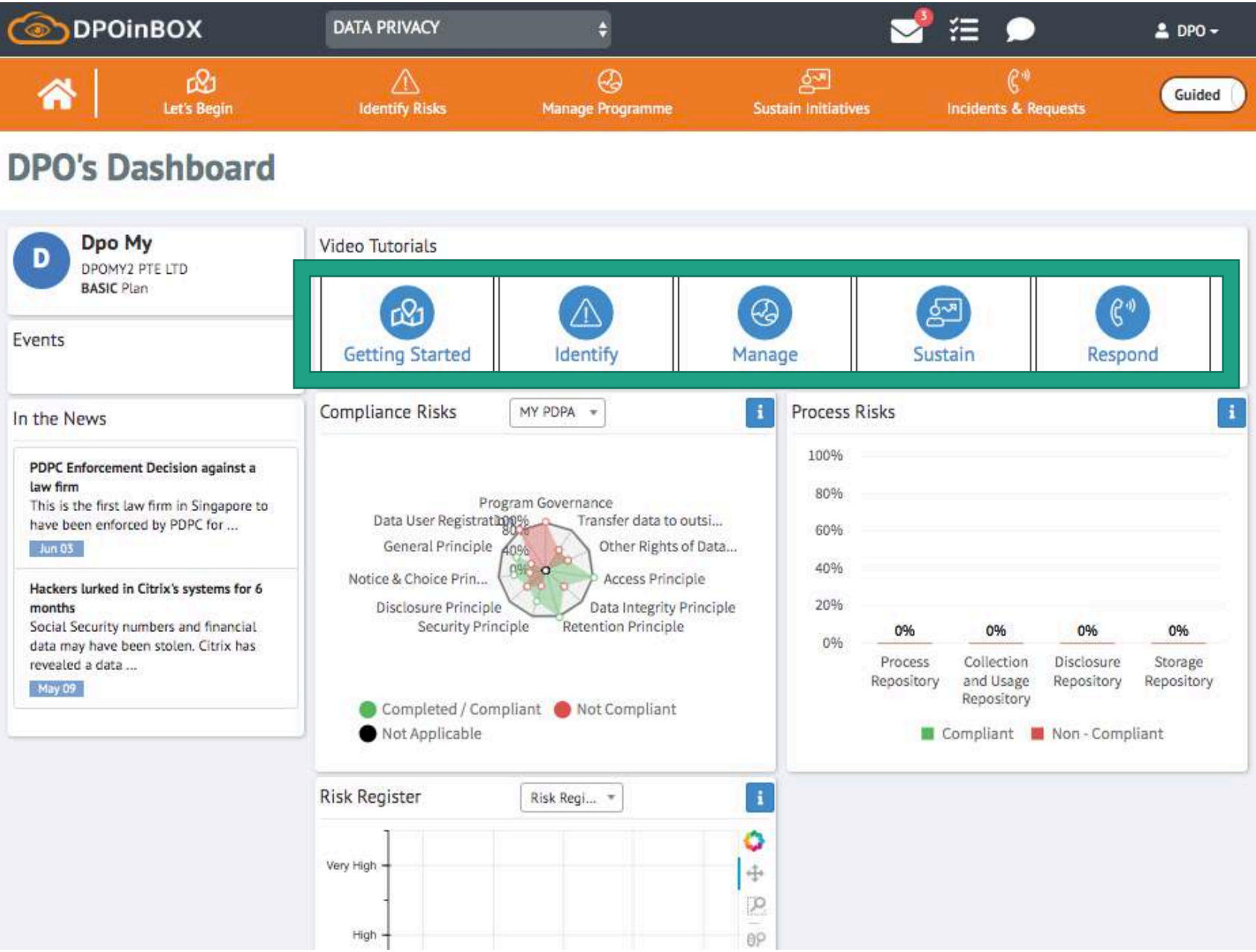
No of employees

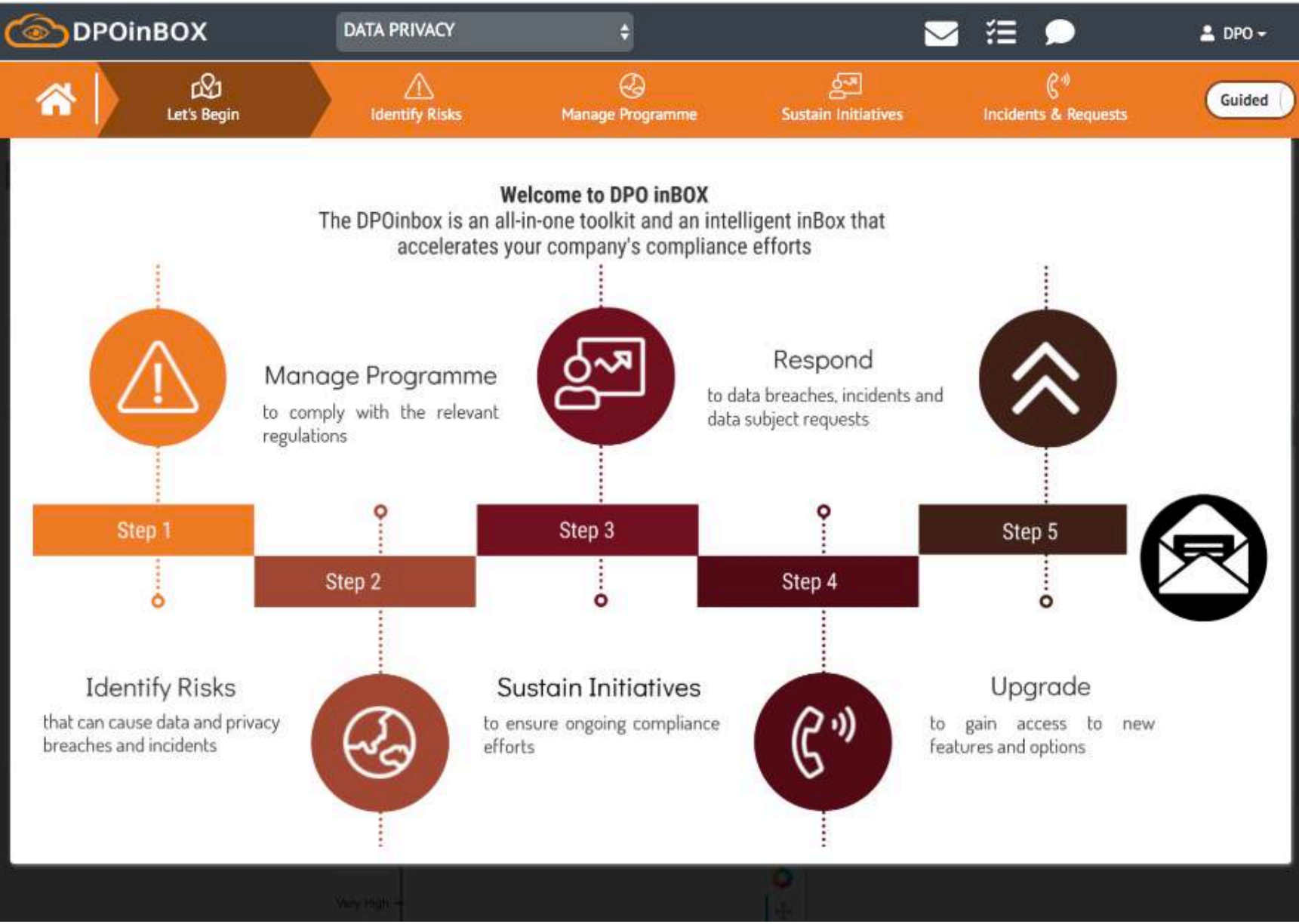
I agree to the terms & conditions*

Your contact details will only be used to assist your compliance journey through the platform as described in our privacy policy.

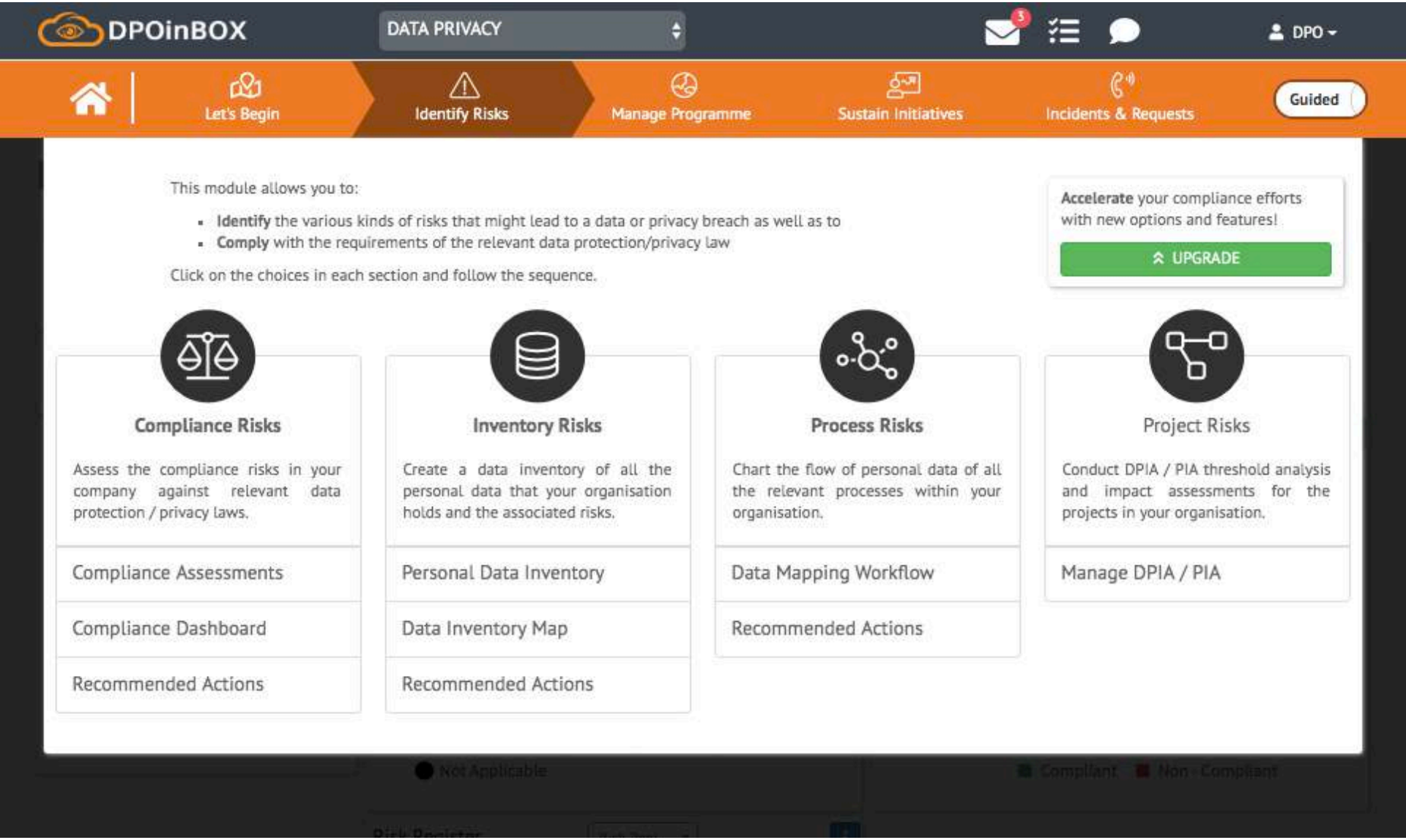
Register

Have an account? Sign in here.

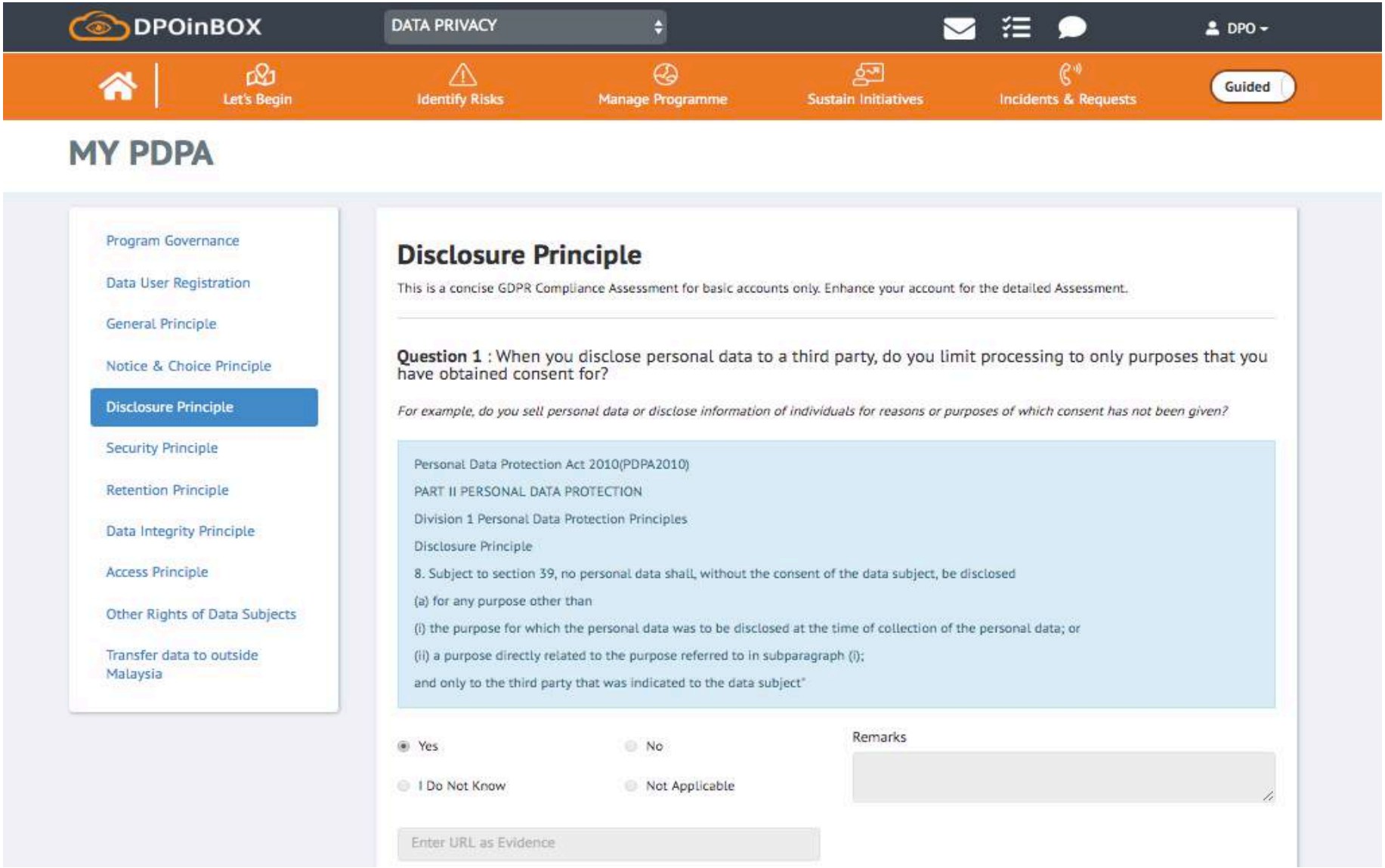

DPOinBOX
DATA PRIVACY
DPO
Let's Begin
Identify Risks
Manage Programme
Sustain Initiatives
Incidents & Requests
Guided
DPO's Dashboard
Dpo My
DPOMY2 PTE LTD
BASIC Plan
Events
In the News
PDPC Enforcement Decision against a law firm
This is the first law firm in Singapore to have been enforced by PDPC for ...
Jun 03
Hackers lurked in Citrix's systems for 6 months
Social Security numbers and financial data may have been stolen. Citrix has revealed a data ...
May 09
Video Tutorials
Getting Started
Identify
Manage
Sustain
Respond
Compliance Risks
MY PDPA
Program Governance
Transfer data to outsi...
Other Rights of Data...
Access Principle
Data Integrity Principle
Retention Principle
Security Principle
Disclosure Principle
Notice & Choice Prin...
General Principle
Data User Registrat...
Completed / Compliant
Not Compliant
Not Applicable
Process Risks
100%
80%
60%
40%
20%
0%
0%
0%
0%
0%
Process Repository
Collection and Usage Repository
Disclosure Repository
Storage Repository
Compliant
Non - Compliant
Risk Register
Risk Regi...
Very High
High

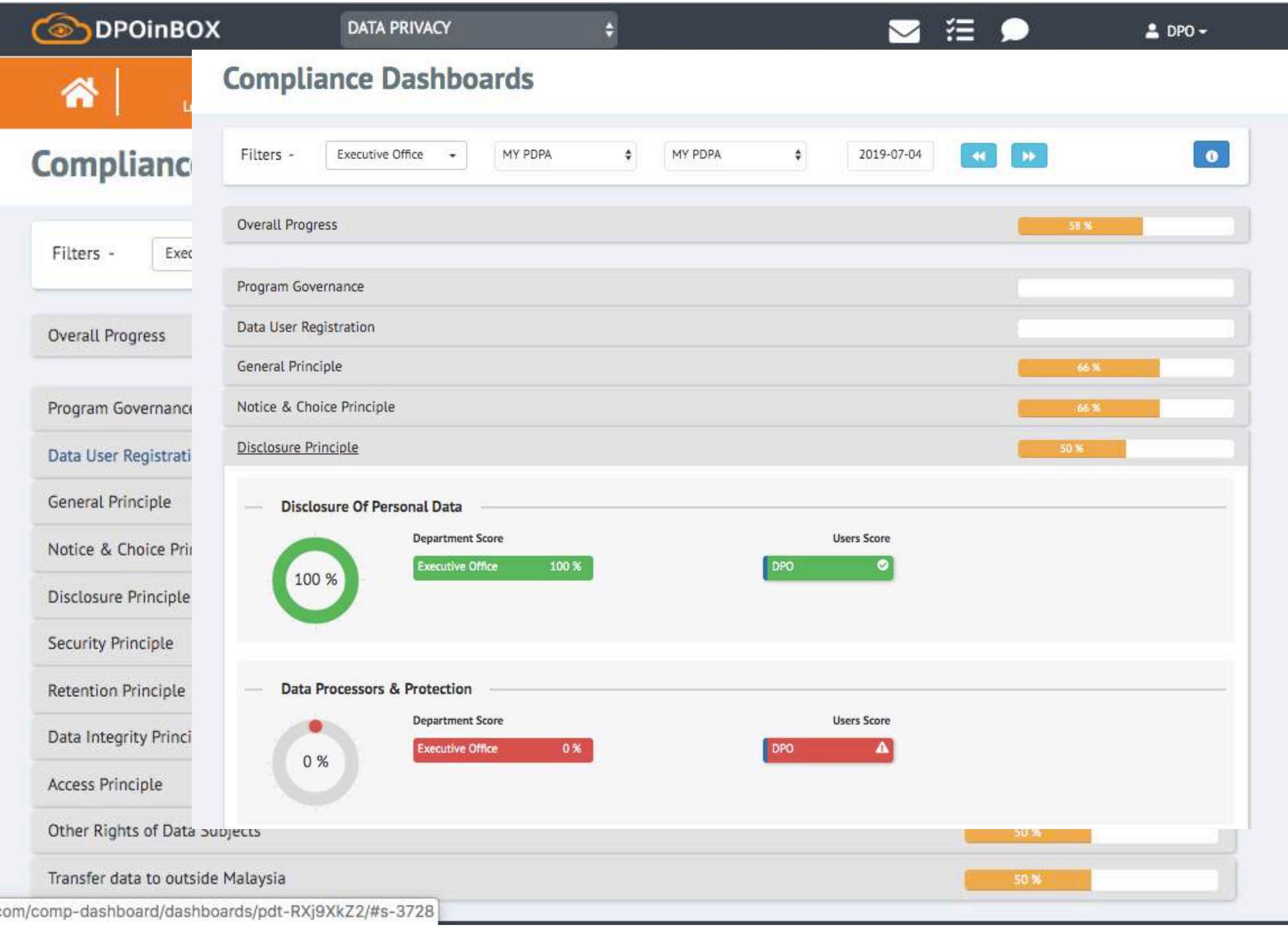

DPOinBOX
DATA PRIVACY
DPO
Let's Begin
Identify Risks
Manage Programme
Sustain Initiatives
Incidents & Requests
Guided
Welcome to DPO inBOX
The DPOinbox is an all-in-one toolkit and an intelligent inBox that accelerates your company's compliance efforts
Manage Programme
to comply with the relevant regulations
Respond
to data breaches, incidents and data subject requests
Step 1
Step 2
Step 3
Step 4
Step 5
Identify Risks
that can cause data and privacy breaches and incidents
Sustain Initiatives
to ensure ongoing compliance efforts
Upgrade
to gain access to new features and options

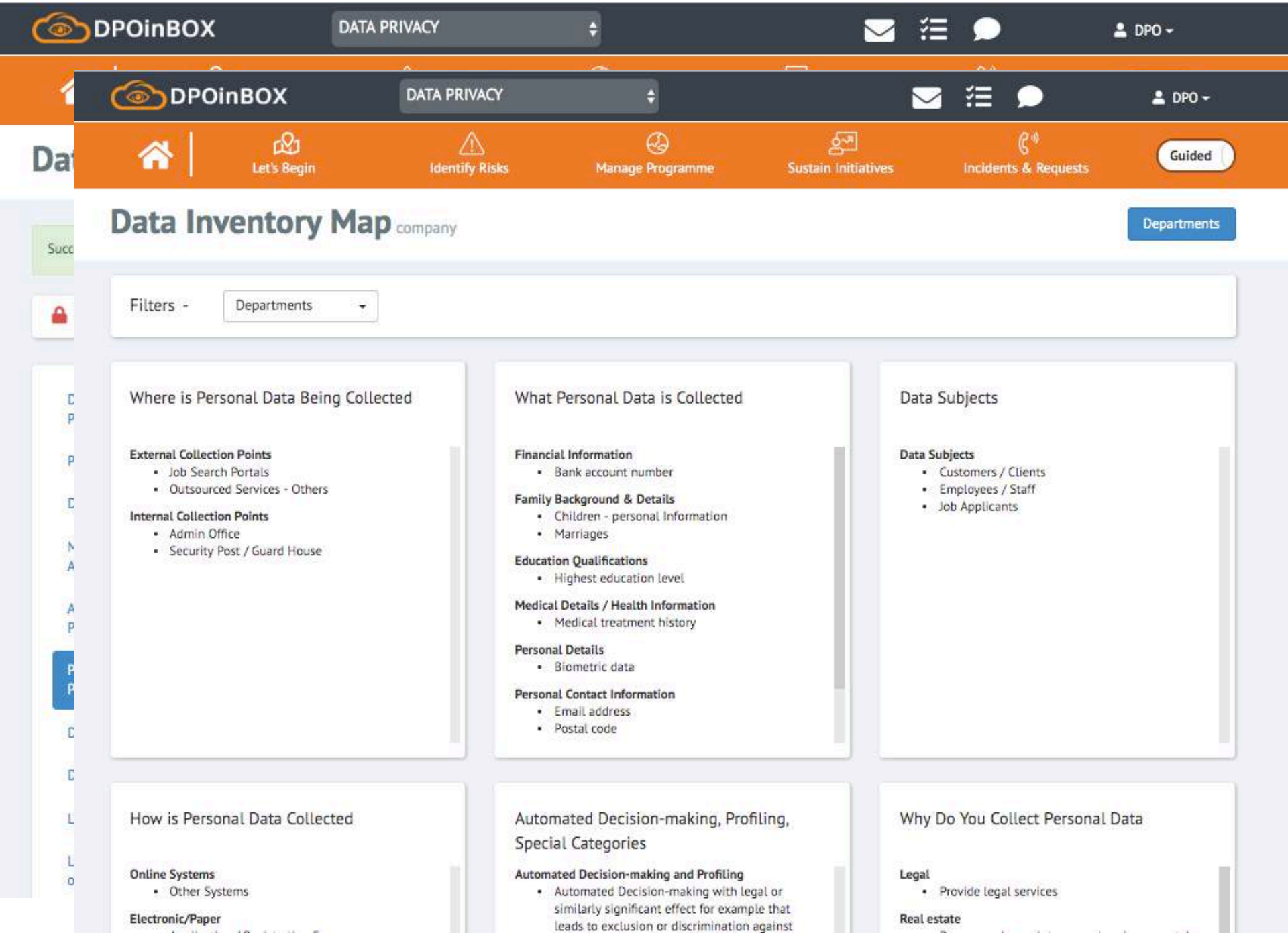
Identify Risk



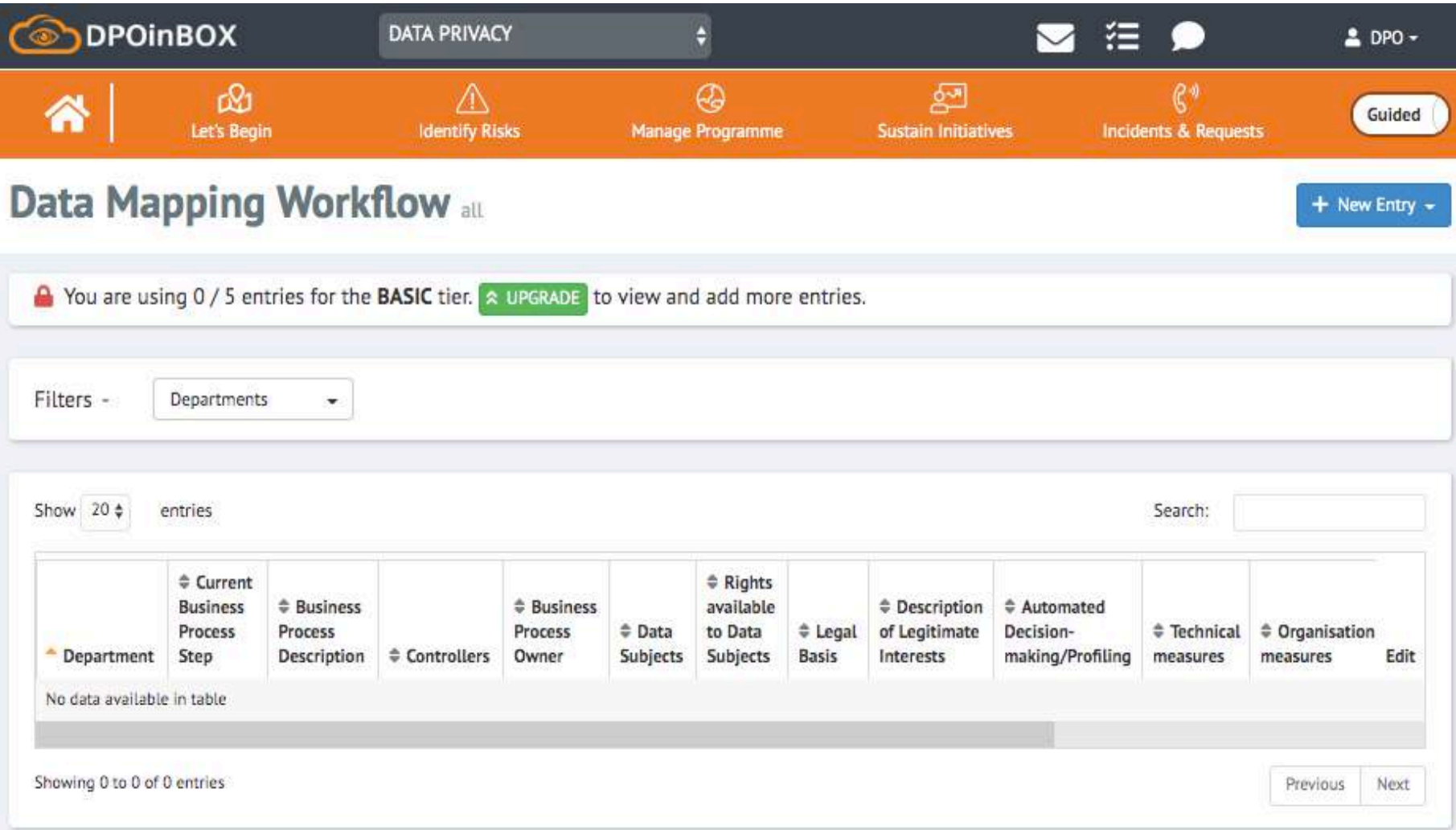
Assessment - Regulation




DPOinBOX
DATA PRIVACY
DPO
Compliance Dashboards
Filters -
Executive Office
MY PDPA
MY PDPA
2019-07-04
Overall Progress
58 %
Program Governance
Data User Registration
General Principle
66 %
Notice & Choice Principle
66 %
Disclosure Principle
50 %
Disclosure Of Personal Data
100 %
Department Score
Executive Office
100 %
Users Score
DPO
Data Processors & Protection
0 %
Department Score
Executive Office
0 %
Users Score
DPO
Other Rights of Data Subjects
50 %
Transfer data to outside Malaysia
50 %
com/comp-dashboard/dashboards/pdt-RXj9XkZ2/#s-3728


DPOinBOX
DATA PRIVACY
DPO
DPOinBOX
DATA PRIVACY
DPO
Let's Begin
Identify Risks
Manage Programme
Sustain Initiatives
Incidents & Requests
Guided
Data Inventory Map company
Departments
Filters -
Departments
Where is Personal Data Being Collected
External Collection Points
Job Search Portals
Outsourced Services - Others
Internal Collection Points
Admin Office
Security Post / Guard House
What Personal Data is Collected
Financial Information
Bank account number
Family Background & Details
Children - personal Information
Marriages
Education Qualifications
Highest education level
Medical Details / Health Information
Medical treatment history
Personal Details
Biometric data
Personal Contact Information
Email address
Postal code
Data Subjects
Data Subjects
Customers / Clients
Employees / Staff
Job Applicants
How is Personal Data Collected
Online Systems
Other Systems
Electronic/Paper
Automated Decision-making, Profiling, Special Categories
Automated Decision-making and Profiling
Automated Decision-making with legal or similarly significant effect for example that leads to exclusion or discrimination against
Why Do You Collect Personal Data
Legal
Provide legal services
Real estate

Data Mapping – Business processes



$17,000+

Average salary increase vs. non-certified counterparts

75,000+

Estimated # DPOs globally to satisfy GDPR requirements

60%

Small businesses that fail within 6 months of a large data incident

81%

Expect minimal/no reductions to privacy staffing post-COVID-19

78%

Report privacy/data protection as a “Board-level” topic

IAPP Resources

- **DPO Toolkit:** https://iapp.org/resources/topics/dpo-toolkit/
- **The Skillset Needed to Implement a Global Privacy Standard:** https://iapp.org/media/pdf/resource_center/ISO_27701_whitepaper.pdf
- **From Here to DPO: Building a Data Protection Officer:** https://iapp.org/media/pdf/resource_center/From_Here_to_DPO_FINAL.pdf
- **The Infosec Professional's Guide to vital Privacy Knowledge:** https://iapp.org/l/infosec-privacy-knowledge/


DPEX
DATA PROTECTION EXCELLENCE NETWORK
About Us · Contact Us
LEARN EVENTS DISCUSSIONS NEWS BLOG RESOURCES PRESS
LOGIN
Welcome to the Data Protection Excellence (DPEX) Network
Asia's Largest Network of Data Protection Officers and Professionals
JOIN OUR COMMUNITY
✓ Training Courses
✓ Case Study Videos
✓ Blogs
✓ Discussion Forums
✓ Events and MORE!!
Join our NEW Data Protection Excellence Network
www.dpexnetwork.org