

Job Positions Requiring Data Protection Expertise

Minimum of 10,000 Data Protection Professionals Needed in Singapore

Research Objective

- Forecast number of data protection professionals needed within the next three years
- Determine if the job market is hiring data protection roles or if job positions have started incorporating data protection expertise as part of the job criteria
- Has there been a change to the above since the Personal Data Protection Commission started enforcements from April 2016?
- Are there any useful insights?

Methodology

- Findings were based on job roles found on respective job portals, *excluding government agencies*.
- Research cover job posts (available job positions) over 2 periods
 - Before the enforcement: July 2016 (Survey was started 3 months after the first enforcement announcements – see <https://www.pdpc.gov.sg/commissions-decisions>)
 - After enforcement: Feb 2017
 - Each survey was conducted within 3 days.
- Key words searched were: “DPO, PDPA, data privacy, data protection, data governance, personal data, sensitive data
- Only job posts where terms relating to data protection were indicated in job description/role, requirements or preference (Skills, experience, qualifications) were included
- Important: data protection could be only one of many other requirements that might be listed in the job posts.

Job Portals Covered

- ✓ Headhunt
- ✓ Indeed
- ✓ Job-q.com
- ✓ JobsCentral
- ✓ Jobstreet
- ✓ LinkedIn
- ✓ Monster
- ✓ RegionUp
- ✓ STJOBS

Executive Summary - 1

Overview

- More than 25 companies have been taken to task for non compliance with the PDPA since the Personal Data Protection Commission first started to fine or warn companies (which started from April 21st, 2016)
- Straits Interactive's research objective was to assess if the PDPC enforcement and market outreach had prompted the job market to require data protection expertise or experience.
- In researching open job positions during in Feb 2017 that referenced data protection either in the job description or requirements, there were a total of 118 of such positions
- This is an estimated 3X more job positions than the previous research done (Jul 2016) (Start of enforcement) where there were only 42 job positions.
- Conclusion is that the PDPC enforcement and market education efforts have prompted more companies to include data protection in their job criteria with regards to regular job roles (besides data protection officer assignments)
- For popular job portals such as Job Street, Monster and Region Up, there was more than a 200% increase in demand for data protection expertise as one job requirement

9/3/17

© Straits Interactive Pte Ltd 2017

Confidential – not for public distribution



Executive Summary - 2

By Sectors

- However, most of the increase for data protection expertise came from the IT sector (24%) and regulated sectors such as financial sector - banking/finance (18%) and insurance (10%).
- Although the IT Sector had the highest percentage of DP-related positions, a significant portion relates to consulting positions and companies with IT security offerings, besides just internal IT functions.
 - Accounting/Auditing/Taxation companies (e.g. the Big 4) have also listed data protection expertise in their consulting positions
- Reference to data protection in the regulated sectors are not surprising given the strong compliance organisational culture. However, lesser regulated sectors (tagged as Others) such as education, hospitality, real estate, retail do not feature prominently. There were only one or two job related positions referencing data protection

Executive Summary - 3

By Job Categories

- The three top job categories are Information Technology (32%), Compliance (22%), Legal (16%).
- While many of the recent breaches relate to info-security, the data in the job posts do not suggest that companies are beefing up their information security or IT practices internally. It appears “business as usual”.
- While the IT job category, like the IT sector earlier, registered the highest number (32%), a large number of the job positions (over 50%) were advertised by companies offering IT products and services.
- This suggests that info-security related companies are leveraging data protection to sell their IT security products and offerings (e.g. Cognizant Technology, Dimension Data Asia Pacific, Gemalto)
- Legal and Compliance make up 38% of all job positions referencing data protection. There has been a significant jump (more than 3X) from the previous research done at the start of the PDPC enforcement. Larger organisations now require data protection as one of the criteria for compliance positions and in-house legal counsels.

Executive Summary - 4

By Data Protection Officers

- Appointing a data protection officer (DPO) is a mandatory requirement under the PDPA.
- Out of the available 118 job positions, 17 listed that a DPO role as either the main role or one of the roles. As expected, the majority of such positions require the applicant to serve dual or multiple roles with DPO as one of the functions.
- It is interesting to note that global brand names - Uber, Facebook, Nike –have dedicated a data protection / privacy office where they have advertised for available positions
- The only local organisations that had job posts related to a dedicated DPO office or role was NUS (Office of Privacy and Compliance) and Great Eastern Life (Regional Data Protection & Governance)

Other departments processing personal data

Number of positions relating to departments that handle personal data such as human resource, finance, marketing were insignificant which suggests the relatively low awareness of incorporating data protection practices in all aspects of the business.

Executive Summary - 5

Comparisons against Cybersecurity and Anti-Money Laundering (AML)

The same search was done on job postings with references to Cybersecurity and AML

- There were 4X more job posts referencing cybersecurity than data protection/privacy. 5X times more - if we compare with AML.
- Cybersecurity is inter-related with data protection. Yet Cybersecurity related positions did not reference data protection or privacy.
- **There will be an estimated 1,000 job roles requiring some sort of data protection experience/expertise** (including DPO roles by end of 2017).
- This is expected to **grow by more than 115% CAGR (compound annual growth rate) to 10,000 over the next three years** depending on the extent of the PDPA fines and new data protection laws being introduced in the region as well as impact of a new law in EU (see later slides for further elaboration)

Implications of Findings - 1

- ❑ Enforcement of the PDPC (25+ companies being warned or fined) and PDPC's awareness campaigns have positively influenced job postings
- ❑ Demand for data protection professionals are gradually growing in demand in Singapore.
 - ❑ However, dedicated DPO roles are still significantly low as Small Medium Enterprises (SMEs) are unable to justify business costs. Multinational corporations (MNCs), companies with regional HQs, and listed companies will likely be those which will be the ones demanding for such expertise
- ❑ However, data protection practices have not been fully operationalised into business functions. These will be prompted by regulatory pressures and demands from partners and consumers overseas and the region.
- ❑ Since there are more job needs related to cybersecurity than data protection, companies need to be aware of different responsibilities required when handling cybersecurity related incidents with personal data breaches with the new Cybersecurity Law to be tabled in Parliament later this year.

Departments that process personal data in a typical SME

- Marketing
- Human Resource
- Finance
- IT

Implications of Findings

- ❑ Companies are ramping up their compliance with local data protection laws and, where they have overseas operations, regional and even European data protection laws. The other driver is company leadership grappling with cyber-security issues.
- ❑ Data protection is to management what cyber security is to technical specialists. They are symbiotic. Data is the new currency and there is a huge opportunity for Singapore to be a regional hub data protection expertise, complementing Singapore's standing as a trusted data hub.
- ❑ How is the demand for data protection expertise being addressed in Singapore? There are only few courses and skills training, leading to a potential shortage.
 - While there has been a greater emphasis on cyber-security skills upgrading among security and IT professionals at the technical level, lesser emphasis has been placed on data protection at the supervisory and management level in terms of re-skilling and training, accounting for the expected the shortage of data protection expertise.
- ❑ Market may reach tipping point when fines imposed on companies start to exceed \$100,000 and when new ASEAN & EU laws are newly introduced or enforced.

Data Protection Related Courses in Singapore

As listed on PDPC's website:

- ❑ **Fundamentals of the Personal Data Protection Act** - two-day course developed under the Business Management Workforce Skills Qualifications (BM WSQ) framework – *for DPOs*
- ❑ **Hands-on Data Protection Officer Training Programme** - Enabling New Competencies for the Data Protection Officer & Complying with the Personal Data Protection Act – 3 day course for DPOs (*DPO competency certificate*)
- ❑ **Certified Information Privacy Manager Programme** (International Association of Privacy Professionals – *IAPP*) – 3 day course for DPOs/Compliance
- ❑ **Certified Information Privacy Technologist Programme** (*IAPP*) – *for Infocomm professionals & developers* - 3 day course for DPOs/Legal professionals
- ❑ **NEW Certified Information Privacy Professional Asia Programme**

Key Stats

Straits Interactive

- Has trained 322 data protection officers (including 81 long term unemployed - LTUs) in 2016 which was an increase from 2015 (70) and 2014 (39)
- There are only an estimated 100 certified privacy managers in Singapore

9/3/17

© Straits Interactive Pte Ltd 2017

Confidential – not for public distribution



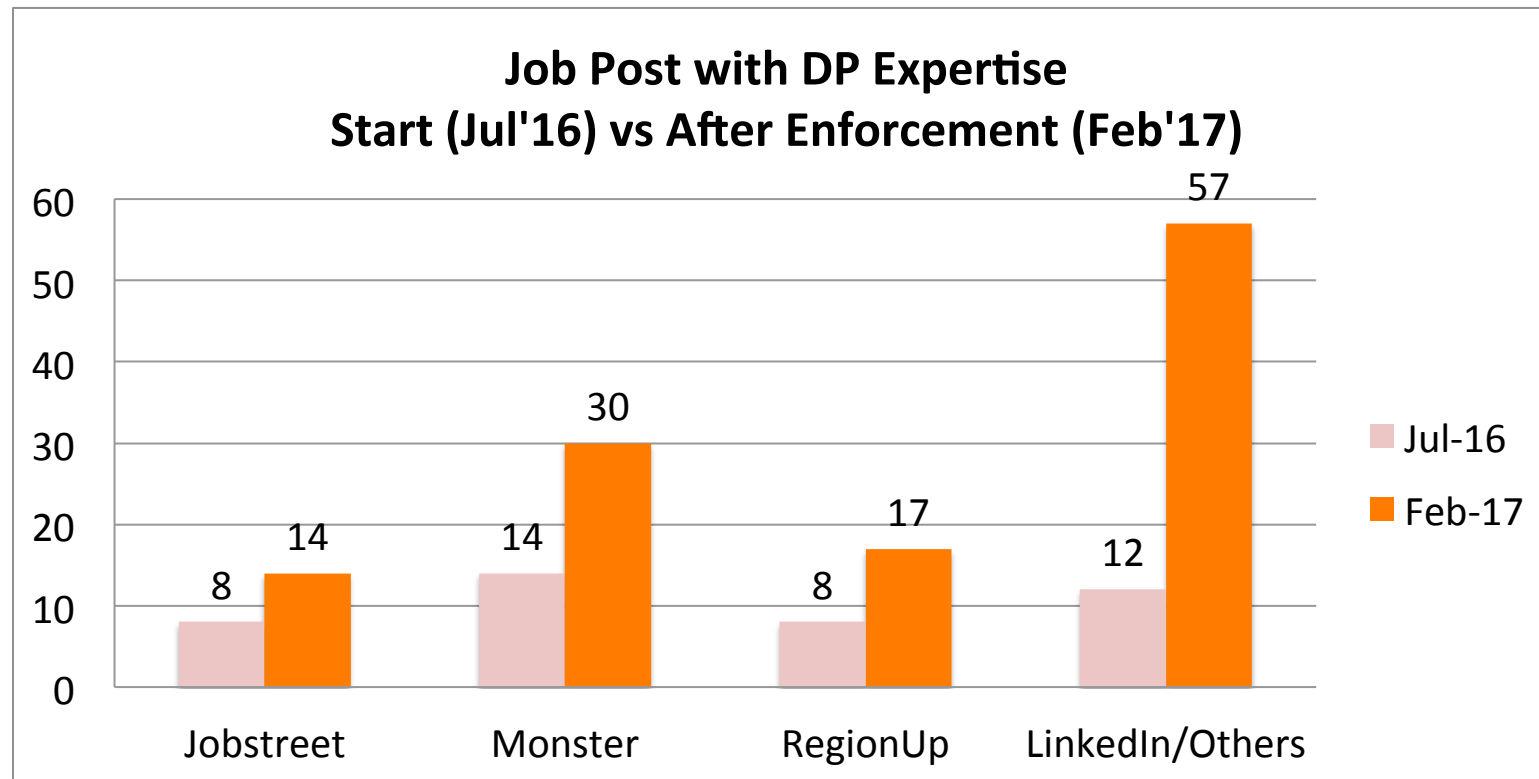
Detailed Report

Comparison of Open Job Positions that Reference Data Protection

2 surveys were taken

- 7th July 16 (3 mths after enforcements were announced) - 42
- 1st Feb 17 (Current status) - 118

For each snapshot, open job positions would have been advertised for as recent as 1 day to as long as 90 days



9/3/17

© Straits Interactive Pte Ltd 2017

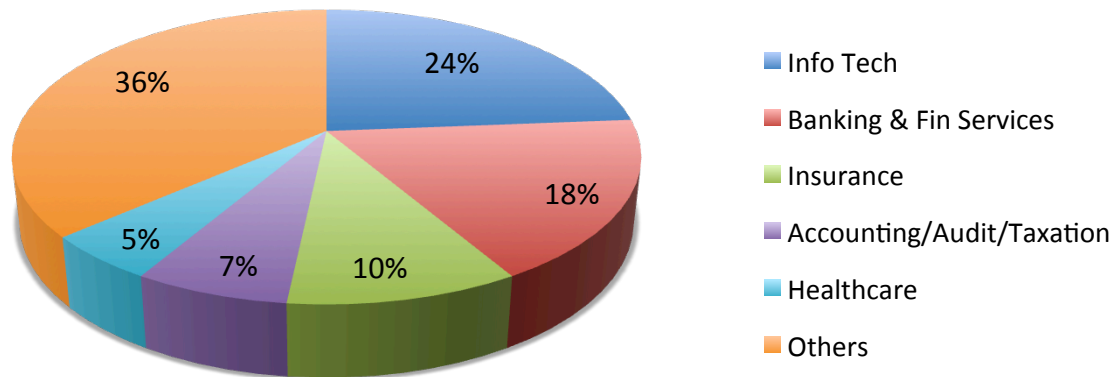
Confidential – not for public distribution



Job positions by Sector

(Feb 2017)

**Job positions with data protection criteria
By Industry**



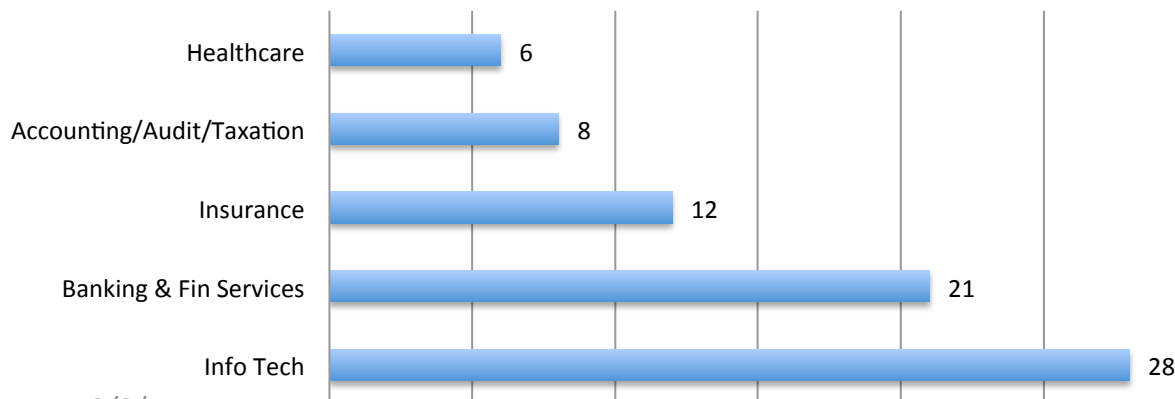
Top 3 industry sectors listing data protection as one of the requirements.

1. Information Technology (24%)
2. Banking of Financial Services (18%)
3. Insurance (10%)

Regulated industries continue to recognise the importance of PDPA.

Accounting/Audit/Taxation refer to companies like Big 4 firms are offerings consulting positions that relate to PDPA.

Job positions with data protection criteria



9/3/17

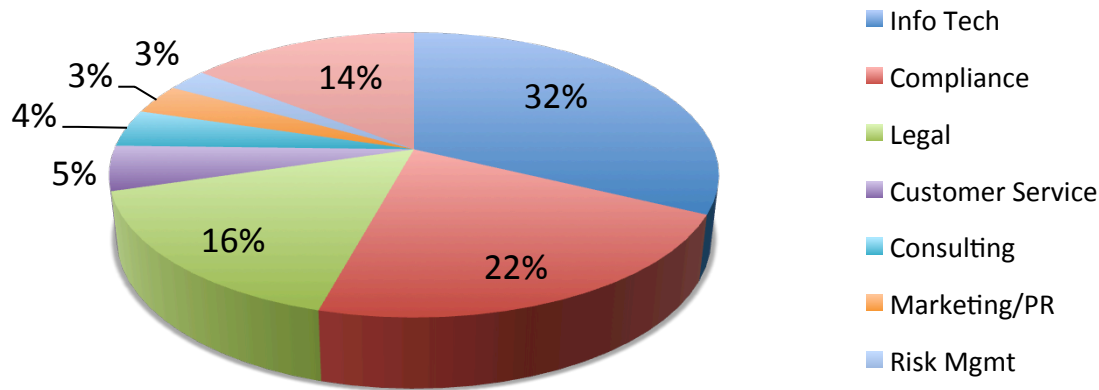
© Straits Interactive Pte Ltd 2017 5 Confidential - Not for public distribution

Job positions by Job Categories

(Feb 2017)

Job positions with data protection criteria

By Job categories



Top 3 job categories listing data protection as one of the requirements

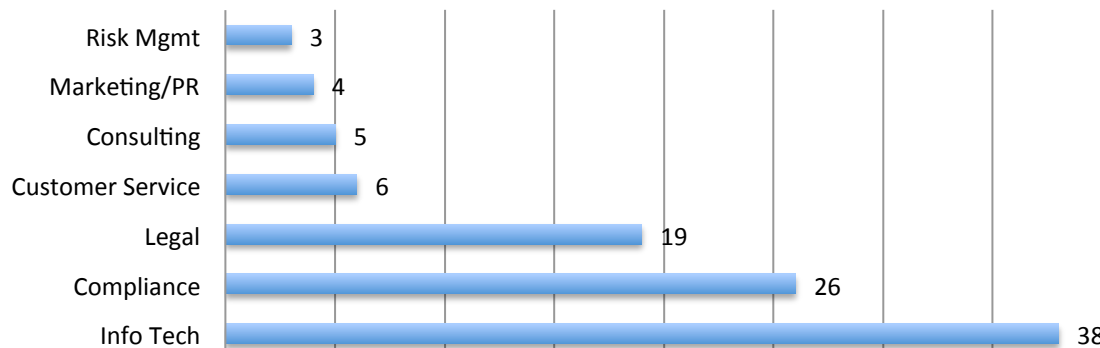
1. Information Technology (32%)
2. Compliance (22%)
3. Legal (16%)

Companies with IT related security offerings are leveraging PDPA to offer consultancy and products

- Half of the info tech roles relate to consulting positions or companies with IT security related products(as opposed to in-house IT departments)

Job positions with data protection criteria

By Job Category



Human resource, marketing and Finance related roles do not feature in the list, although these job categories involves processing of personal data

Job positions by Job Categories

Job_Categories	Number of job positions
Information Technology	38
Compliance	26
Legal	19
Customer Service	6
Consulting	5
Marketing/Public Relations	4
Risk Management	3
Education/Training	2
Admin/Secretarial	2
Human Resources	2
Business Development	1
General Work	1
Healthcare/Pharmaceutical	1
Logistics/Supply Chain	1
Others	1
Professional Services	1
Project Management/ Information Technology	1
Sales/Retail	1
Sciences/Laboratory/R&D	1
Security & Investigation	1
Healthcare/Pharmaceutical	1

Examples of job positions relating to Information Technology

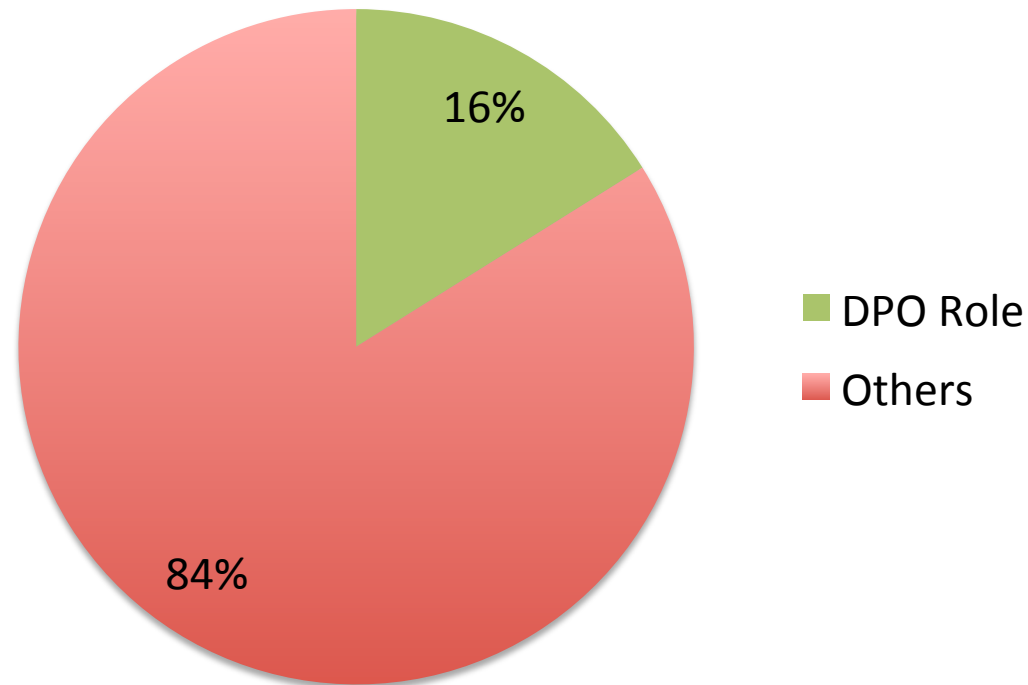
- Cognizant Technology Solutions Asia Pacific Pte Ltd (provides digital, technology, consulting, and operations services.)
- Dimension Data Asia Pacific Pte Ltd (information technology services)
- Itcan Pte Limited (Technology service and solutions company)
- Gemalto (international digital security company)
- Nutanix (The enterprise cloud company making datacenter infrastructure)
- Dataspark (Data Scientists)

A significant number of positions are from companies leveraging data protection to sell their security products and offerings as opposed to internal IT functions.

Data Protection Officer Roles

(Feb 2017)

Job posts requiring a DPO

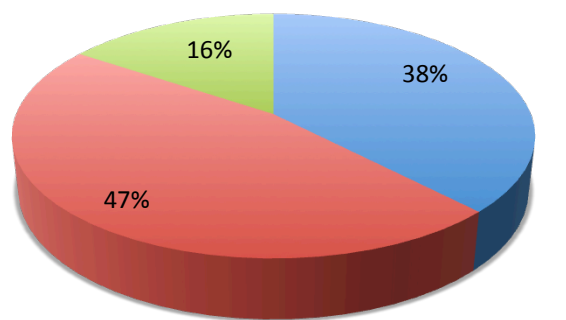


Out of the 118 available job positions which reference data protection, only 17 (16%) lists the role of data protection officer or involves a position in the data protection office or supporting one.

International brands - Uber, Facebook, Nike - have dedicated data protection / privacy office. Only local organisation with dedicated DPO office or role is NUS and Great Eastern Life.

Job positions by Job Experience

(Feb 2017)



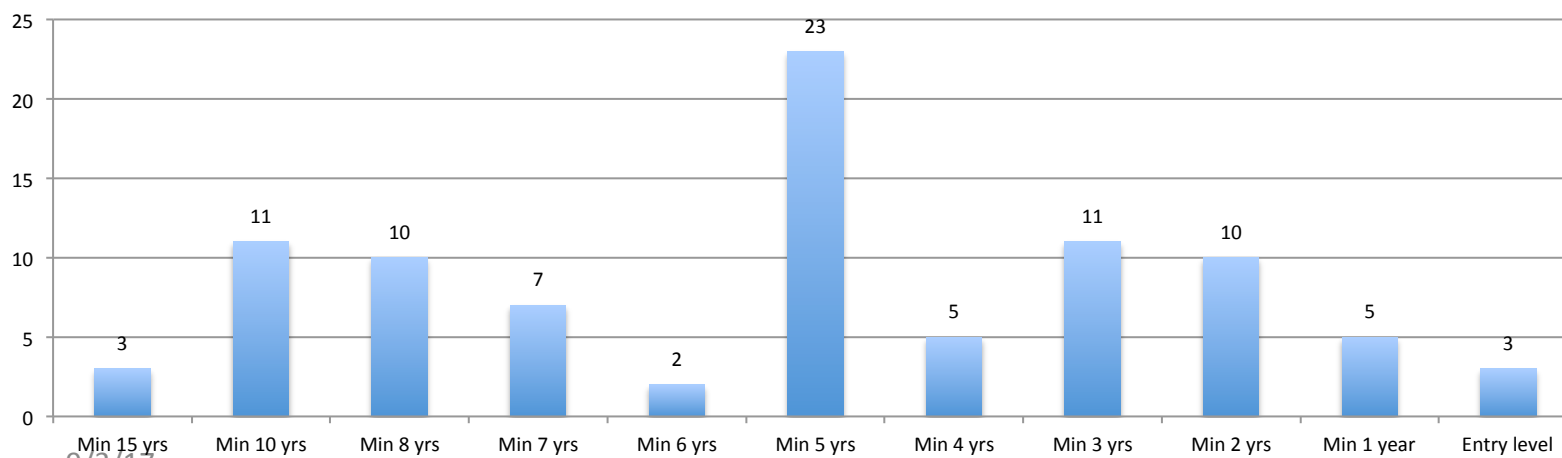
Below 5 years 5 - 10 years Above 10 years

Only 90/118 of the open job positions listed minimum years of experience required.

At least 63% of the job posts require minimum of 5 years work experience.

This is because individuals need to understand the business processes of the organisation in order to contribute in the area of data protection.

Distribution of Min Job Experience



Job positions vs Cybersecurity & AML

(Feb 2017)

References made			
Job_Portal	Data Protection	Cyber-Security	AML
Jobstreet	14	137	171
Monster	30	124	79
RegionUp	17	41	142
LinkedIn	57	166	181
Total	118	468	573

- ☐ Compared to Cybersecurity and AML (Anti Money Laundering), the field of data protection is still relatively new
- ☐ As a comparison, **there were 4 times more job posts referencing cyber security than data protection/privacy**. 5 times more if we compare with AML
- ☐ Using the above numbers as a guide, **by year end, there would be an estimated 1,000 job roles requiring some sort of data protection experience/expertise** (including DPO roles).
- ☐ This is expected to **grow by more than 115% CAGR (compound annual growth rate) to 10,000 over the next three years** depending on the extent of the PDPA fines and new data protection laws being introduced in the region as well as impact of a new law in EU (see later slides for further elaboration).

Sample Extracts found in Job posts

9/3/17

© Straits Interactive Pte Ltd 2017

Confidential – not for public distribution



DPO Position - Samples

- To **develop data protection policies** and ensure that it is consistently implemented across [organisation].
- To provide advice and guide the various departments to align business processes to **comply with the PDPA**.
- Manage and respond to patients/participants queries and requests in a timely manner according to the **PDPA response framework**.
- You will **organise meetings for the Data Protection Officer (DPO) workgroup** and conduct presentations to senior management.
- Direct [organisation's] **strategy on privacy policy** and data-driven innovation for the APAC region.
- Analyze legislative and **regulatory proposals concerning privacy**, data security and related technology issues.
- Review organization's **personal data inventory** and processes to flag out potential **data protection risks**, via periodic risk assessment.
- **Develop personal data policies**, including drafting relevant SOPs, and oversee organization's **compliance with PDPA**.
- **Understanding of data security, privacy, data protection**, regulatory and compliance procedures

9/3/17

IT Position - Samples

- Experience in IT security, compliance and risk management, including **privacy**, controls, etc.
- Good knowledge of information security solutions including identity and access management, **privacy and data protection**, application security, server security, network security, vulnerability management and/or cryptography.
- Actively monitor new and emerging security and **privacy related technologies**, trends, issues, and solutions and assess their applicability.
- Create and maintain processes that are **PDPA Compliant** for the database and safeguard the privacy of the data.
- Deep understanding of **data protection technologies** like replication, snapshot, backup, restore, etc.
- Perform all functions of an enterprise NAS environment including **data protection**, backups, archiving and snapshots, de-duplication and replication.
- Play a key role in the bank's data leakage prevention program to proactive monitor and **protect its data**.
- To review and approve the implementation of **Data protection plans** and designs.
- To provide **data protection technology** integration support cradle to grave: predeployment through deployment and post.

IT Consultant - Samples

- Responsibility for the creation of key Information Security Intelligence, Risk and **Privacy** and/or Cloud Security assets, Security Analytics, Information Security Architecture to be used by the security practice globally.
- Detailed understanding of regulatory frameworks and **data protection legislation**.
- Knowledge in Security solutions including Firewall, Content Security, Intrusion prevention, encryption, data leakage, **data protection** and monitoring security will be added advantage.
- Security-related certifications such. As CISSP, CRISC, GIAC, CIPP, RSA, CCNE, ISO 27001 LA, CISA, CISM and knowledge of regulatory guidelines such as ISO 2700x standards, **data protection** are desirable.
- **Design and develop data protection solutions** using [company] products deployed into customer environments where sensitive information needs to be protected.

Legal Job Position - Samples

- Experience conducting or supporting corporate internal investigations, with a sound understanding of legal privilege, **data privacy** and other related legal issues.
- Provide appropriate best-in-class end-to-end legal commercial, regulatory and compliance advice, **including data protection advice** (with reference to the **Data Protection Counsel**) on customer, partner, accountant and procurement matters.
- You will advise on a broad spectrum of legal issues arising from their trading activities. Functions include: corporate, commercial, M&A and **data protection**, regulatory compliance issues, commercial negotiations etc.
- Acting as key tech lawyer for the business, advise on all tech-related matters including ecommerce, **data privacy**, regulatory compliance and IP/IT.
- Substantive knowledge and demonstrated expertise in **APAC privacy** and consumer protection laws.
- Substantive knowledge of **EU data protection framework**

Compliance Job Position - Samples

- **Resolve privacy**, tax, contracts, employment and other barriers.
- Providing regulatory compliance advisory to the business on a wide range of issues including but not limited to, compliance issues, risk, sales governance, **data privacy**, outsourcing.
- Other Experience Will Be Of An Advantage - Knowledge in **Privacy and Data Protection**.
- Ensure that controls around **data privacy policies** are adhered to during new product launches and for existing products.
- You will be the subject matter expert of Information Governance Policy and **PDPA (Personal Data Protection Act)**, raising awareness, advisory and provide guidance in the matter.
- You possess sound knowledge and experience in **PDPA**, records management/ document control in an engineering discipline.
- Provide Regulatory Advisory support to client and Service delivery team around Monetary Authority of Singapore (MAS) requirements, Association of Bank in Singapore (ABS), **Personal Data Protection Act (Singapore)**, Cyber Security and Computer Mis-use Act.

10,000 Data Protection Professionals needed in Singapore within next 3 years

9/3/17

© Straits Interactive Pte Ltd 2017

Confidential – not for public distribution



More than 10,000 Data Protections Professionals needed within next 3 years

7 Reasons Why

1. All companies and other businesses operating in Singapore must comply with the PDPA;
2. The PDPA mandates appointment of at least one DPO;
3. The PDPC is actively enforcing the PDPA with more than 25 companies getting into trouble so far;
4. More countries in the region are introducing data protection laws and countries that already have them are increasing their enforcement activity;
5. Organisations in the region, including Singapore, must comply with new European data protection law from early 2018 if, for example, they market their goods or services to Europeans;
6. Continued high profile data breaches worldwide;
7. Smart Nation Vision and Singapore's digitalisation drive.

Data Protection Officer is a Mandatory Requirement under the PDPA

“All business, big or small, requires a Data Protection Officer (DPO). This is someone who can develop and implement good policies and practices for handling personal data that meets the organisation’s needs; someone who can communicate policies and practices clearly to employees and customers; and someone who can manage personal data-related queries or complaints.”

Source: Personal Data Protection Communication Advertisement, 2016

New data protection laws are being introduced or enforced in ASEAN

“ASEAN has committed to harmonise legal infrastructure for e-commerce in the Roadmap for Integration of the e-ASEAN Sector. One of the targets in the Strategic Schedule for the ASEAN Economic Community (AEC) is to adopt best practices/guidelines on various cyber law issues including data protection.

Singapore, Malaysia and the Philippines are the only countries with dedicated data protection laws; Indonesia and Thailand have circulated draft data protection laws. It is important to watch this space as the bill goes through the legislative process.”

Source: Rouse the Magazine: Data Protection in ASEAN, 4 July 2016



New data protection rules in Europe affect everyone

“The EU's new data protection rules that are expected to become law in 2018 will impact every entity that holds or uses European personal data both inside and outside of Europe, according to legal experts. A key element of the General Data Protection Regulation (GDPR) is that it not only gives rise to increased compliance requirements, but these are backed by heavy financial penalties, which in the final text turned out to be up to €20m or 4% of annual worldwide turnover for groups of companies, whichever is greater.”

Source: Computer Weekly World, Jan 11, 2016

Study: GDPR's global reach to require at least 75,000 DPOs worldwide

“Earlier this year, an IAPP study conservatively estimated that, once the GDPR takes effect, at least 28,000 DPOs will be needed in Europe and the United States alone. Applying a similar methodology, we now estimate that as many as 75,000 DPO positions will be created in response to the GDPR around the globe.”

Source: International Association of Privacy Professionals, Nov 9, 2016

Confidential – not for public distribution

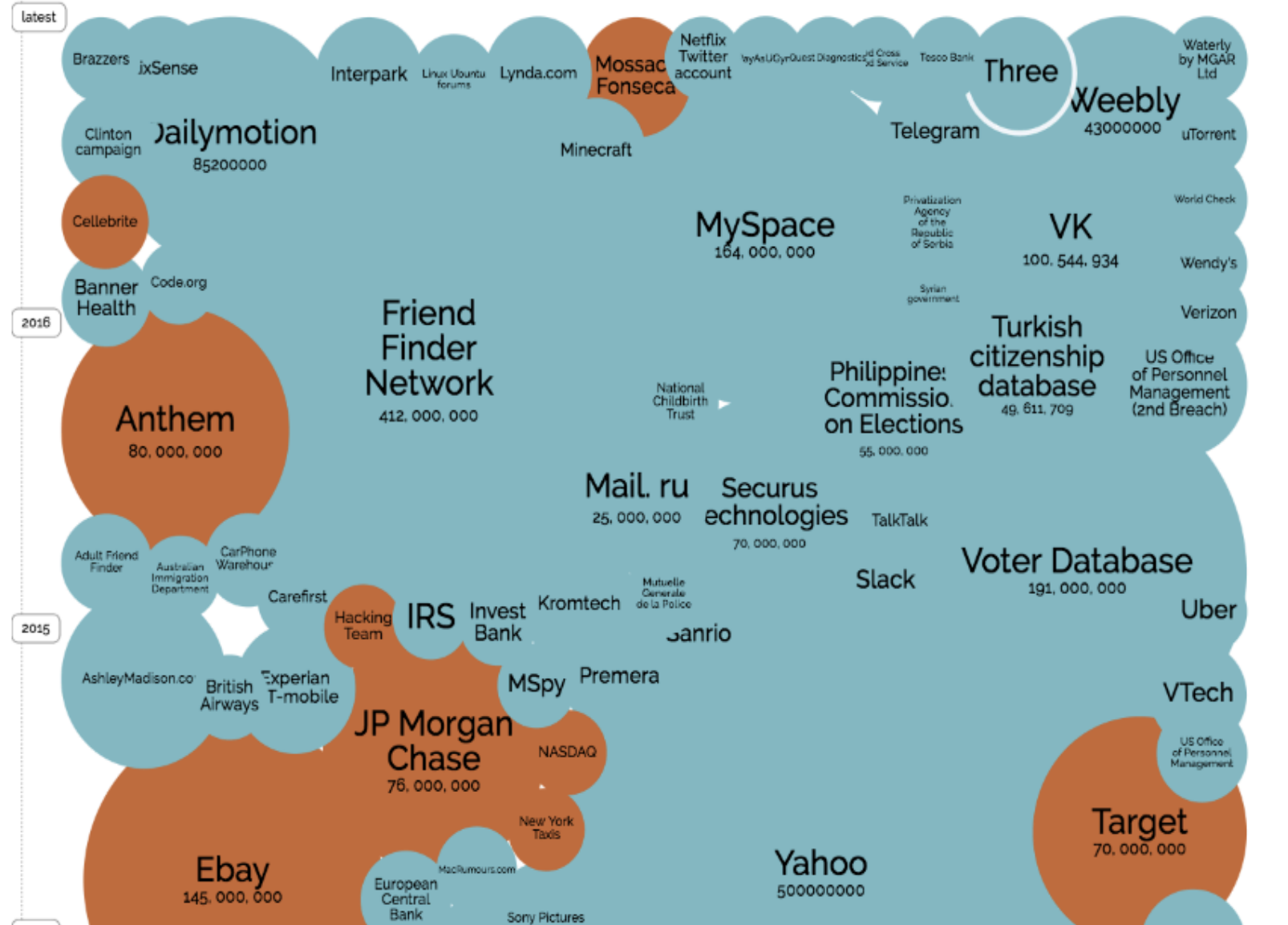


World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 5th Jan 2017)

interesting story

YEAR BUBBLE COLOUR YEAR METHOD OF LEAK BUBBLE SIZE NO OF RECORDS STOLEN DATA SENSITIVITY SHOW FILTER



Survey of Top 100 Local Apps (vs Global Survey)

Summary findings from Singapore's first privacy survey covering mobile applications
Conducted by straits interactive with support from app knox (28 Oct 2016)

	Global Apps	OPC Apps*	SG Apps
Total # of apps examined	1211	151	103
Permissions (Indicator 2)			
Apps requesting 1 or more permissions	75%	70%	89%

Permission Requested

	Global Apps	OPC Apps	SG Apps
Location	32%	22%	70%
Contacts	9%	10%	7%
Calendar	2%	2%	8%
Microphone	5%	7%	4%
Camera	10%	8%	29%
Device ID	16%	13%	52%
Access to other accounts	15%	23%	49%
SMS	4%	6%	12%
Call log	7%	11%	2%

*OPC – Officer of the Privacy Commission, Canada

Key Observations

- 89% of Singapore's mobile apps requested >1 permission, higher than global average
- In terms of permissions, Singapore has a higher average in 6 of the 9 permissions surveyed worldwide - Location, Calendar, Camera, Device ID, Access to Other Accounts, SMS

As Singapore moves towards its vision of becoming a Smart Nation, companies developing or deploying apps for their customers and users will need to address and strengthen the privacy elements of their apps," said Mr. Ken Chia, Principal, Baker & McKenzie.Wong & Leow. "They may not realise the privacy implications of their actions and that they may be contravening the Personal Data Protection Act. There is thus a need to further strengthen privacy in the face of an open world and a good way to do that is to help our technologists understand how privacy and security work hand in hand."

https://www.straitsinteractive.com/PR_SI_Mobile_Apps_Survey_28102015.pdf

9/3/17

© Straits Interactive Pte Ltd 2017

Confidential – not for public distribution



Singapore's Smart Nation Vision

Innovation and the advent of big data analytics rely significantly on the creative collection and use of data, including **personal data**. In the past decade, we saw the rapid adoption of e-commerce, social media, and mobile devices and applications that utilise data to facilitate convenience in daily lives and enhance connectivity for communications and productivity.

It is difficult to argue against the benefits of innovation and new opportunities that such developments bring, but it is also **important to ensure that the element of trust must be maintained** for users and stakeholders of such technologies. **How Singapore and the Personal Data Protection Commission define this issue will affect the ability and limits of innovators.**

Source: Keynote Speech by Mr Leong Keng Thai, Chairman of PDPC, at the 6th European Data Protection Days Conference, Monday, 25 April 2016, in Berlin, Germany

We will also **strengthen our capabilities in data and cybersecurity**. With increased digitalisation, data will become an important asset for firms, and strong cybersecurity is needed for our networks to function smoothly. The Cyber Security Agency (CSA) of Singapore will work with professional bodies to train cybersecurity professionals.

Source: Budget 2017, Budget Speech

Digitalisation

Digital technology has unique potential to transform businesses, large and small, across the economy. The first way to strengthen our enterprises, especially SMEs, is to help them adopt digital solutions.

SMEs Go Digital Programme

We will introduce the SMEs Go Digital Programme to help SMEs build digital capabilities.

Validating the Forecast...

9/3/17

© Straits Interactive Pte Ltd 2017

Confidential – not for public distribution



Key Stats & Indicators

Overall

- 302,537 foreign and local (Pte Ltd) companies operating in Singapore (Source: ACRA, Nov 2016)
- 640 mainboard listings and 134 catalyst listings on the Stock Exchange (Wikipedia - as for Jan 2010)
- 11,000 European companies in Singapore (Source: Ministry of Finance)
- 2210 start-ups with regional or global ambitions (angel.co)

Banking and Financial Services

- 126 Commercial banks (5 local, 121 foreign)
 - 400 fund management companies
 - 181 licensed insurers
- (Source: MAS)

Other entities that process personal data

- 6751 F&B Establishments (Dept of Statistics & Spring Singapore)
- 3713 Employment Agencies (MOH Search)
- 2215 registered charities (Office of the Commissioner of Charities - COC - Dec 27, 2016)
- 1519 Maid Agencies (FDW - Foreign Domestic Workers)
- >1000 travel agencies – STB – May 4, 2016
- 927 printing companies with 15440 workers (Spring Singapore – 2013)
- 398 hotels in Singapore (STB - Dec 2016)
- 228 security agencies (SPF - May 31st 2016)

Personnel / Agents processing personal data

- 20,000 - 30,000 Number of financial advisor practitioners
- 30423 - real estate agents (CEA)
- Estimated 30,000 HR professionals (WDA - Apr 2016)
- 33,000 Security personnel (ST – 13 May 2016)
- 6000 developers - mobile, web site, social media (IMDA projections – ST 26 Jan 2016)
- 2150 – Certified InfoSec Professionals (ISACA)

9/3/17

Methodology

How we arrived at the numbers

Consider the following facts:

- There are **302,537 foreign and local** (Pte Ltd) companies operating in Singapore (Source: ACRA, Nov 2016).
- 190,000 of them are estimated to be SMEs (Small Medium Enterprises) (Source: Spring Singapore). They employ about 70 per cent of the workforce. SMEs refer to enterprises with not more than \$100m in annual revenues or employ not more than 200 employees;.
- Fact check: According to ACRA, 186,577 companies were **assessed for corporate income tax** (ACRA: YA2015) – to ensure that we cover only active companies.
- If we use this number as a benchmark, it means that ***as many 190,000 active companies must appoint a data protection officer.***
- In our calculations, we assume that only the larger and profitable enterprises will be motivated to hire either a dedicated DPO or more likely assign a DPO role to an existing function (e.g. Compliance, HR, IT, or marketing, etc.).

Methodology

Chargeable Income Group S\$	Number of Companies	Chargeable Income S\$'000	Net Tax Assessed S\$'000
10,000 & below	16,658	56,052	6,780
10,001 - 20,000	7,112	104,712	12,935
20,001 - 30,000	6,839	176,878	24,360
30,001 - 40,000	3,758	130,812	16,191
40,001 - 60,000	5,401	266,689	32,846
60,001 - 80,000	3,942	273,998	33,797
80,001 - 100,000	3,056	274,104	33,786
100,001 - 150,000	4,955	610,559	75,351
150,001 - 200,000	2,249	390,621	51,261
200,001 - 300,000	2,636	651,381	78,786
300,001 - 400,000	1,744	605,476	73,208
400,001 - 500,000	1,314	588,997	71,147
500,001 - 1,000,000	3,565	2,491,291	319,563
1,000,001 - 2,000,000	2,439	3,447,473	504,105
2,000,001 - 3,000,000	1,081	2,652,992	405,613
3,000,001 - 4,000,000	576	2,001,348	308,887
4,000,001 - 5,000,000	394	1,760,125	276,119
5,000,001 & above	2,200	92,163,508	11,269,033
Total	69,919	108,647,016	13,593,767

Source: IRAS

- Hence, if we assume only the companies that paid taxes in YA2015, **this number drops to 69,919, where we omitted loss-making companies.**
- We further filtered the numbers to only companies that made chargeable income of more than **\$100,000 as a condition**, assuming companies in this chargeable income group would have the means to invest in PDPA compliance
- **Hence, the number we arrived was 23,153 companies.**

9/3/17

Methodology

- Next we **removed two key industries** from the overall numbers:
 - Information & Communications
 - Financial & Insurance Activities
- Companies in the financial sector would likely already have a data protection officer because of the strong compliance culture as a result of MAS regulations.
- We also assumed that companies in the information and communications sector would likely have relatively higher security measures and may not be as vulnerable to a data breach as compared to other sectors.
- These 2 sectors make up 17% of all companies (source: IRAS). Hence, if we only took 73% of the **23,153 companies**. **This will further reduce the number to 16902 ($0.73 \times 23,153$).**

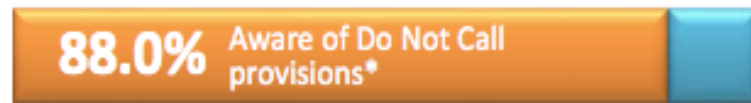
2016 Industry Survey on the Personal Data Protection Act (PDPA)

Conducted between March and June 2016 among 1,513 companies of various industry sectors and sizes



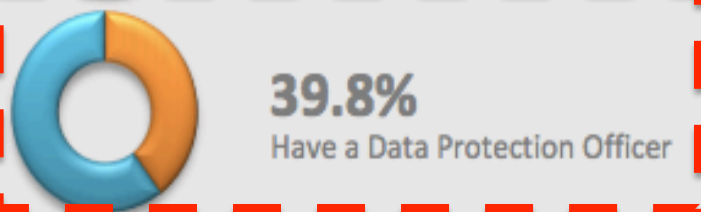
Organisations in Singapore are generally aware of their need to protect the personal data of customers and employees. However, some may require more assistance in the implementation of their data protection policies.

AWARENESS OF THE PDPA



*Of those that conduct telemarketing activities

COMPLIANCE OF THE PDPA



We then applied a formula from a PDPC survey done in 2016 (sample size: 1513) which revealed that 39.8% of companies had already appointed a data protection officer.

$$(0.6 \times 16902) = 10,141$$

Hence, we estimated that a minimum number of 10,000 DPOs/DP Expertise.

9/3/17

The End