DLA PIPER

# GLOBAL DATA PRIVACY SNAPSHOT 2018:

## How does your organisation compare?

## Introduction

Data protection is rising on the agenda globally: the past year has seen China introduce the PRC Cybersecurity Law, the introduction of Australia's mandatory Privacy Amendment (Notifiable Data Breaches) Act 2017, while the EU's long awaited General Data Protection Regulation is due to come in to force in May 2018.

## DLA Piper's Data Privacy Team & Scorebox

DLA Piper's Data Protection group launched the 'Privacy Scorebox' tool in January 2016 to help organisations to address their privacy compliance challenges in different jurisdictions. The complimentary tool takes the form of a survey which poses a series of questions relating to the 12 areas of data privacy that feature most prominently in data protection legislation around the world, such as storage of data, use of data, and customer rights. At the end of the survey, respondents are awarded a percentage score, which reflects their alignment with these key principles.

## 2018 Privacy Snapshot

The inaugural Privacy Snapshot whitepaper, published in January 2017, examined the responses of the approximately 250 respondents who completed the Scorebox survey between January and December 2016.

This, the second Snapshot whitepaper, examines the responses of the over 200 organisations who completed the survey during the calendar year 2017. The data analysed provides insight into their approaches to the key privacy principles, examining the percentage scores awarded to each respondent.

## Summary of findings

The average alignment score for respondents in 2017 was 34.4%, which means that while many organisations have rigorous processes in place, many still have gaps in more than one area.

While some sectors, and some revenue size groups fared better than others, average scores for each were all under 40%.

## GDPR deadline approaching

For many organisations, time is pressing to conduct a thorough audit of processes and implement a plan for data protection compliance.

Organisations with operations in the European Union will by now be aware that the General Data Protection Regulation (GDPR) will start to apply from 25 May 2018. It will apply to all entities operating in the European Union, whether or not they are established in the EU.

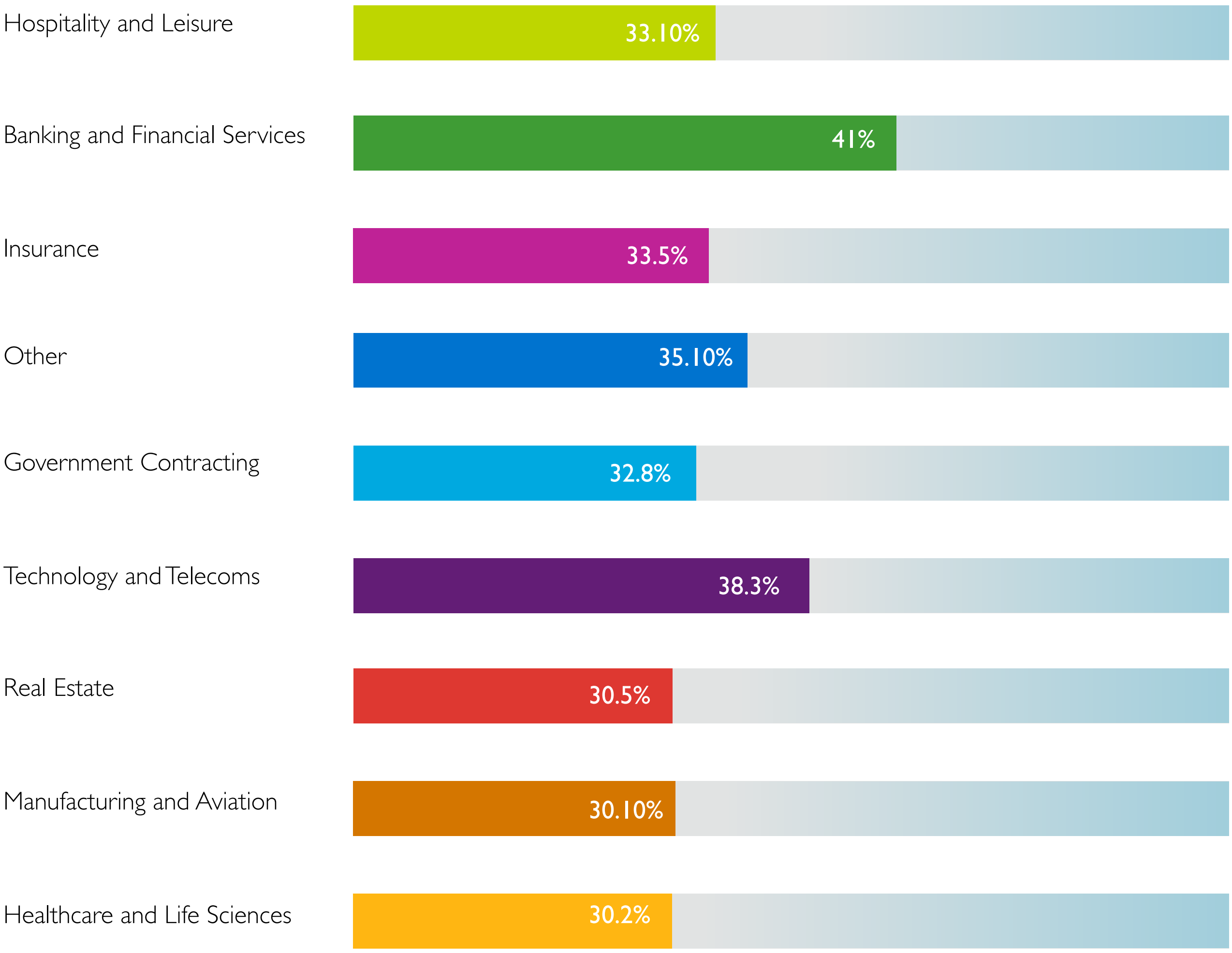
The GDPR introduces new, more stringent requirements in the field of data protection, and stiff penalties for those organisations that do not comply. The clock is now ticking, with heavy fines for those who fail to comply with the requirements of GDPR. Organisations have a great deal to do between now and 25 May to prepare for the new regime.

# OVERVIEW OF FINDINGS

An overview of the alignment of organisations - spanning different sectors, sizes and geographies - to key global data protection principles.

## Average alignment percentage score for all companies surveyed: 34.4%

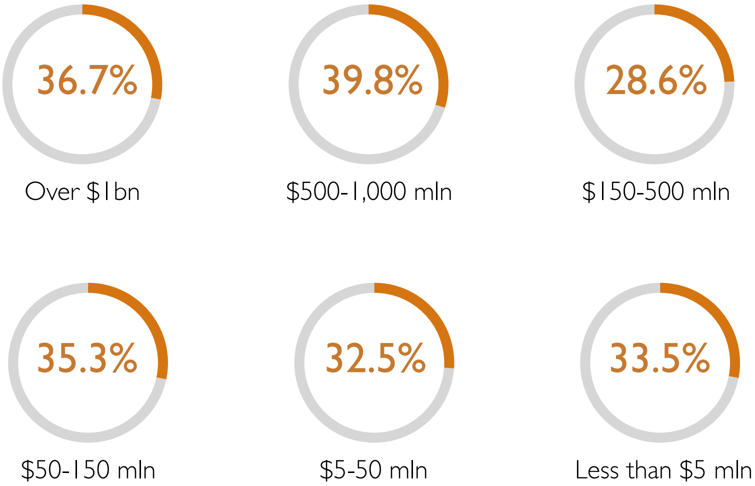
Average score per sector:



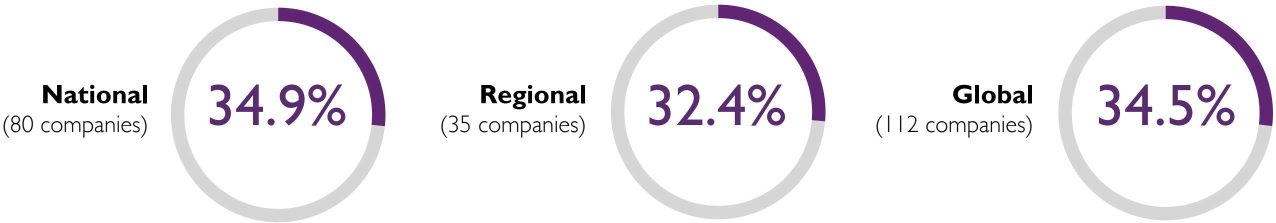
# OVERVIEW OF FINDINGS

An overview of the alignment of organisations - spanning different sectors, sizes and geographies - to key global data protection principles.

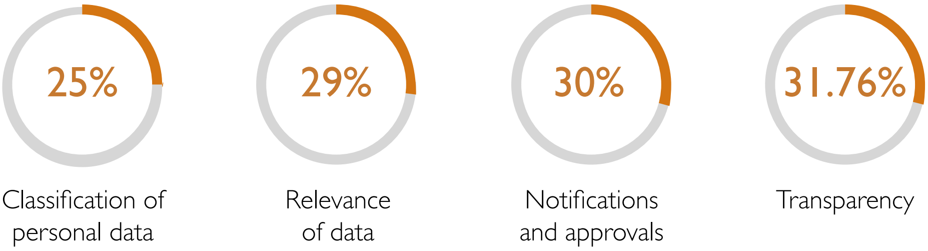
Average score per revenue size group:



Average score per reach



Areas where respondents scored lowest average score



# HEALTHCARE & LIFE SCIENCES

## Key recommendations based on common responses:

### Privacy policies

Make sure that you have privacy policies in place that you issue to customers/ staff, explaining how you process their personal data: organisations must be transparent about how they process personal data, providing a clear notice to individuals, typically in a privacy notice, policy or statement.

### Classification of personal data

Make sure that you classify data into a 'sensitivity' type, allowing you to stratify and manage risk for different categories of data: data protection laws often identify special categories of personal data which require additional protection - for example, financial data, health data, judicial data, information on an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, criminal history, trade union membership or sex life.

### Relevance

Make sure your organisation regularly validates whether personal data records remain accurate and up-to-date. Only collect as much information as you strictly need to support each activity mentioned in the privacy policies and put processes in place to ensure you stick to this guiding principle.

### Notifications and approvals

Ensure that you have checked the position in each market where you operate and have up to date notifications and approvals in place with all the relevant authorities.

# HEALTHCARE & LIFE SCIENCES

## Right to process data

ONLY **29%**

have a strict process in place to map out the basis on which they collect personal data

## Data Storage

**35%**

said that generally data storage is decided based on commercial factors such as pricing, and that privacy and data protection rules are not really considered

ONLY **23%**

say that privacy and data protection risk is always considered as part of any decision

## Right to access, rectification, deletion and objection

**41%**

don't have any formal procedures to manage these requests and are not sure if they would (technically) be able handle them

## Notification and approvals

**35%**

are missing notifications/ approvals in one or more countries where they know they ought to have these in place, or where they may be out of date

## Relevance

**41%**

do not specifically regulate how much information they collect about people

## Privacy Policies

**59%**

have privacy policies covering some (but not all) of the business functions that routinely process personal data

## Data Classification

**35%**

do not distinguish between different types of personal data and generally treat all types of data in the same way

## Cross border transfers

**53%**

make cross-border transfers but are not sure if the transfers comply with specific rules that regulate these arrangements

## Accuracy of records

**41%**

do not routinely validate their records to ensure databases are accurate and up-to-date

# FINANCIAL SERVICES

## Key recommendations based on common responses:

### Use of personal data

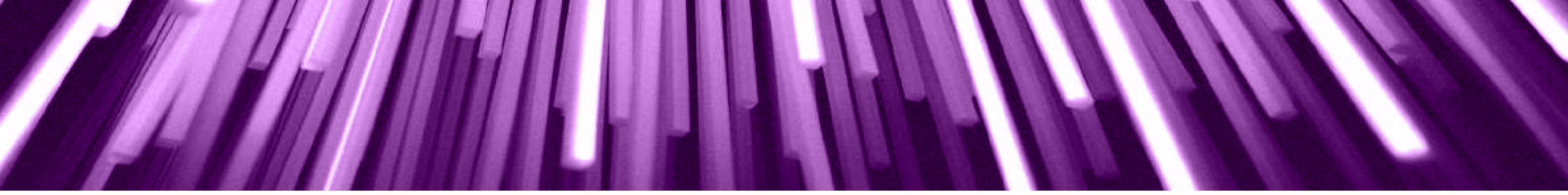
Ensure you have a clear understanding about the purposes for which you want to use personal data, in advance of collecting it from the individual: in most countries personal data can only be processed for the explicit purposes contained in the privacy notice (or for purposes which are compatible with those initial purposes).

### Accuracy of records

Make sure your organisation regularly validates whether personal data records remain accurate and up-to-date. Only collect as much information as you strictly need to support each activity mentioned in the privacy policies and put processes in place to ensure you stick to this guiding principle.

### Individuals' rights to access, rectify, delete and object

Make sure you have procedures in place to allow individuals to access a copy of their data files (or arrange for any errors to be corrected/ irrelevant details removed) upon request



# FINANCIAL SERVICES

## Security standards

**21%**

apply a single set of security standards to all data types

**ONLY 21%**

have a graduated set of security standards which reflects a range of situations / data types

## Relevance

**52%**

don't specifically regulate how much information they collect about people - generally they keep what they can as it may be helpful in the future

**ONLY 15%**

collect as much information as they strictly need to support each activity mentioned in the privacy policies and have processes in place to ensure they stick to this guiding principle

## Accuracy of records

**ONLY 5%**

have robust processes in place to regularly check and update data records to ensure they remain accurate and up-to-date

## Intra-group

Of respondents that have more than one establishment, 50% have not set out a clear plan as to how data should be shared within their different group companies.

**ONLY 7%**

maintain a register which clearly shows what each group company is authorised to do with the various data processing operations that they carry out

## Right to process

**47%**

do not routinely analyse the legal basis on which they collect, use and share personal data

## External transfers

**47%**

don't have any formal processes in place for external transfers and generally don't consider privacy risk in these situations

## Individual's rights to access, rectify, delete

**ONLY 21%**

have adopted procedures into their systems to allow them to easily respond to requests for access, rectification, deletion and objection

**26%**

don't have any formal procedures to manage these requests and are not sure if they would (technically) be able handle them

# TECHNOLOGY

## Key recommendations based on common responses:

### Relevance of data

Make sure your organisation regularly validates whether personal data records remain accurate and up-to-date. Only collect as much information as you strictly need to support each activity mentioned in the privacy policies and put processes in place to ensure you stick to this guiding principle.

### Individuals' rights

Make sure you have procedures in place to allow individuals to access a copy of their data files (or arrange for any errors to be corrected/ irrelevant details removed) upon request.

### Internal organisation awareness

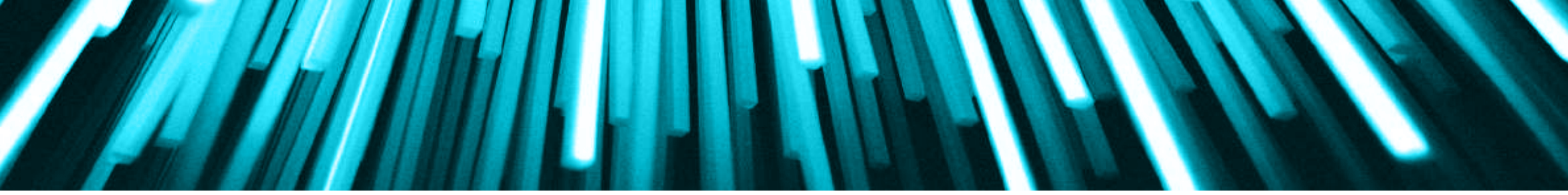
Make sure you have internal standards, procedures, guidelines, etc. to guide employees in the collection, use and sharing of personal data.

### Internal standards

Consider employing an individual whose role is dedicated to privacy and data protection within the organisation ('data protection officer'). In some countries, it is mandatory to have a data protection officer. Even in countries where this is not legally required, the appointment of a data protection officer can be considered as best practice. Note that it is not always required that this person is exclusively dedicated to data protection.

### Employee training

Ensure that employees receive training regarding data protection and refresher sessions as required.



# TECHNOLOGY

## Accuracy

**38%**
do not routinely validate their records to ensure databases are accurate and up-to-date

**48%**
update records only on an ad hoc basis if they become aware of inaccurate or outdated data file

## Data storage

**24%**
say that generally data storage is decided based on commercial factors such as pricing etc. Privacy and data protection rules are not really considered

A further **38%** say that privacy and data protection risk is taken into account, but only for more strategic projects

## External transfers

**40%**
don't have any formal processes in place and generally don't consider privacy risk in these situations

**42%**
have basic processes in place to manage data sharing with other organisations, but the processes are not consistently applied

## Security classification

**36%**
apply a single set of security standards to all data types

A further **40%** have a graduated set of security standards, however these are based on technical standards only

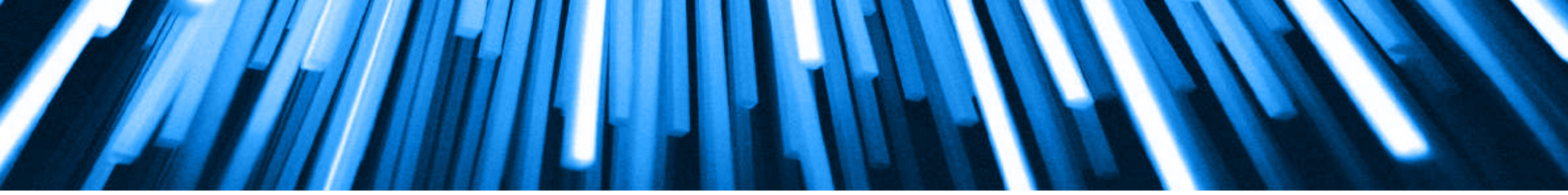
## Data classification

**40%**
do not distinguish between different types of personal data and generally treat all types of data in the same way

## Rights to access, rectify, delete or object

**16%**
don't have any formal procedures to manage these requests and are not sure if they would (technically) be able handle them

ONLY **16%**
have adopted procedures into their systems to allow them to easily respond to these requests



# ABOUT THE REPORT & METHODOLOGY

## About the Data Privacy Scorebox

An online data protection tool, the Data Privacy Scorebox is designed to assist clients with assessing and benchmarking the data privacy maturity level of their organisation.

The complimentary tool takes the form of a survey which poses a series of questions relating to 12 areas of data privacy, such as storage of data, use of data, and customer rights.  It takes no longer than half an hour to complete, with a range of multiple choice answers from which to select.

The Data Privacy Scorebox was launched on Data Protection Day in January 2016.This report examines responses from the over 200 organisations to have completed the assessment in the 2017 calendar year (for 2016 results see the January 2017 Privacy Snapshot report).

We have analysed the data and produced a report which sets out to provide a snapshot of the data protection maturity of these leading businesses and organisations, to give a cross-sector view.

These organisations have turnovers ranging from less than 5 million to over 1 billion pounds/dollars, and are either national, regional or global in presence.

## About the DLA Piper Data Protection Practice

DLA Piper's Data Protection, Privacy and Security group comprises over 150 lawyers worldwide who provide consistent, practical, business-friendly legal advice around highly sophisticated data management, data security and privacy law to achieve effective compliance, across a range of sectors, wherever our clients do business.

The group has played a major role at the forefront of the development of privacy, data security breach and data security laws around the world. Our data protection team has successfully worked together in recent years to assist more than 250 multinational organizations in the design and implementation of global privacy and security programs.

**2017 Privacy Snapshot report**

**Find out more:**
**www.dlapiper.com/dataprotection**

**or contact**
**dataprivacy@dlapiper.com**

DLA PIPER