DLA PIPER

GLOBAL DATA PRIVACY SNAPSHOT 2017:

How does your organisation compare?

DLA PIPER

Personal information is an increasingly valuable business asset. Technology provides the opportunity to understand and engage with customers and stakeholders like never before. Deployed carefully, it can enhance relationships and provide tangible competitive advantage in the marketplace. It needs to be managed with care, as collecting, using and sharing data is subject to increasing levels of regulation by legislators concerned about personal privacy and cyber attacks.

Changes to EU Data Protection Law

The European General Data Protection Regulation (GDPR) which comes fully into effect in May 2018 will herald some of the most stringent data protection laws in the world, imposing a heightened compliance regime underpinned by ramped-up enforcement including the potential for fines of up to 4% global corporate turnover.

DLA Piper's Data Privacy Team & Scorebox

The DLA Piper Data Protection, Privacy and Security group provides market leading legal guidance and support to prepare many of the world's largest businesses for the GDPR. We launched the Privacy Scorebox to enable organisations to assess their current levels of privacy maturity relative to industry peers, giving us in return a unique insight into how the market is performing.

One year after launch, the Scorebox's multi-national, multi-sector data from over 250 organisations is the most comprehensive resource currently available to track levels of privacy compliance in the business world.

Summary Findings

The responses collected through the Scorebox show a general awareness about GDPR across almost all businesses, and the enhanced regulatory regime that needs to be managed. Awareness is high, but levels of maturity to meet the new standards are low. Almost all responding organisations have significant work to do.

In the sections below we provide further insights into how businesses within three core sectors fare based on the Scorebox data. We will monitor the Scorebox results to see how current levels change prior to GDPR implementation.

Key Recommendations

Take a strategic approach to compliance. Rather than focus on ad hoc issues, plan ahead to understand the full scope of requirements imposed by GDPR and work out a strategic plan that secures effective implementation for May 2018.

Be aware of your vulnerabilities. Take time to identify, manage and remedy gaps. Through careful assessment and planning, risks arising from more innovative business activities involving the use of personal data, or expanding global operations, can be readily identified and managed.

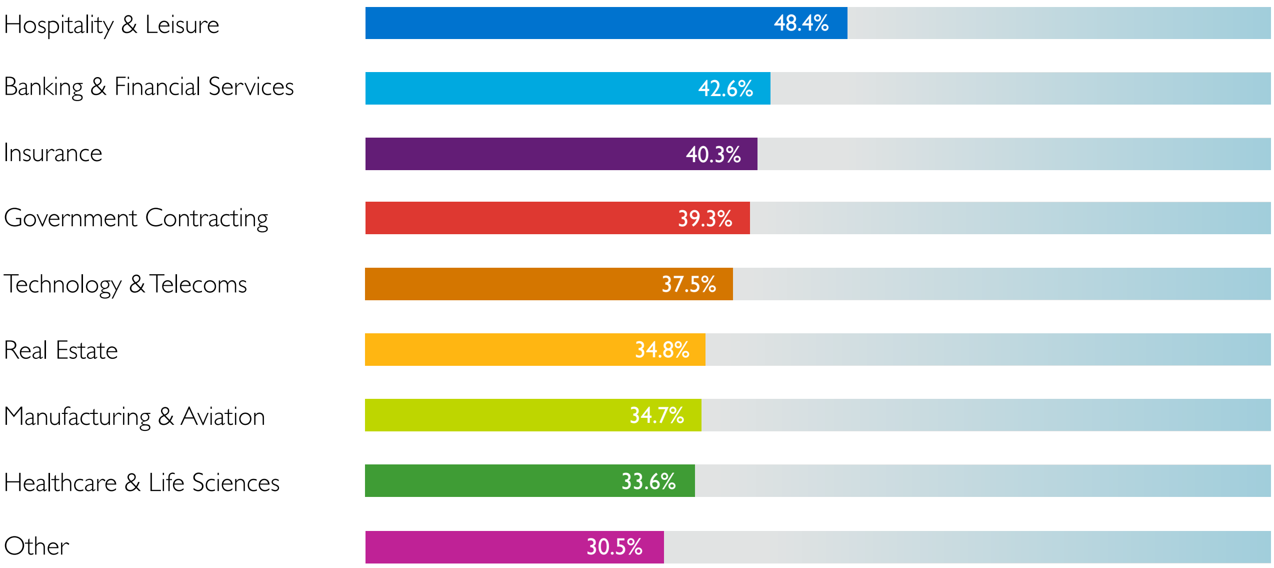
Prepare stakeholders now for the challenges ahead. Successful compliance depends upon support across the business stakeholder community. If they understand the possible sanctions of non-compliance to the business and more importantly the benefits and opportunities of managing data effectively, stakeholders will be supportive, putting the organisation on an effective track to compliance.

The clock is now ticking. The Scorebox results show most organisations have a lot to do. Investing in data privacy has never been more critical. Those organisations focusing on compliance now will give themselves the best possible lead time to meet the challenge of the new regime and be at the forefront of the opportunities presented in the digital economy.

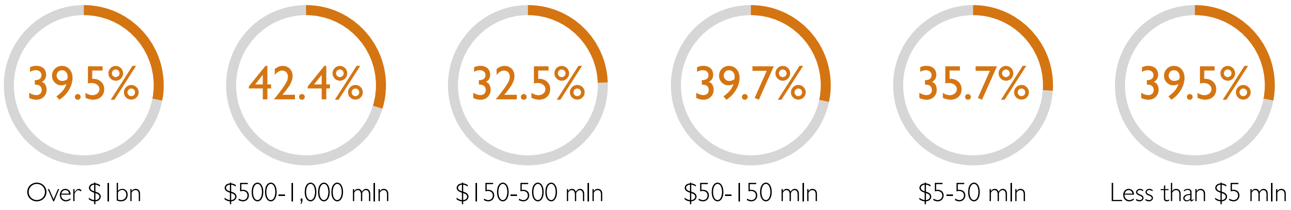
OVERVIEW OF FINDINGS

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

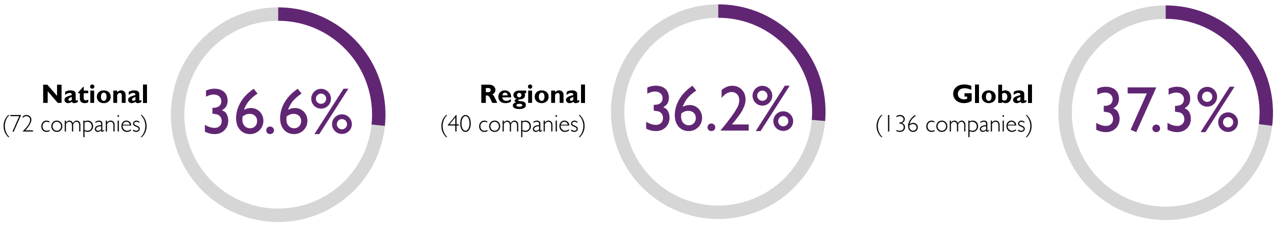
Average score per sector:



Average score per revenue size group:



Average score per reach:



HEALTHCARE & LIFE SCIENCES

The Healthcare and Life Sciences sector has always been heavily regulated in certain areas, due to the sensitive nature of data in relation to, for example, drug trials. Attention is now turning to the management of data in other areas of the product life-cycle.

The last few years have seen an explosion of healthcare innovations which empower patients and enable healthcare professionals to do their work faster and more efficiently. However, they also necessitate enhanced data collection and careful management of that data by the different organisations in the healthcare process.

The responses we have received to date from the sector indicate that organisations are aware of their GDPR obligations, and are planning accordingly. The challenge now will be to ensure that they have completed that process ahead of the implementation date.

HEALTHCARE & LIFE SCIENCES

Privacy Policies

25%

of organisations have privacy policies in place for all business functions which routinely process personal data.

3 out of 5

created bespoke policies to match actual processing operations.

Right to process data

50%

of organisations often ask individuals to provide consent when collecting data, but do not have a formal process for tracking why and how this data is asked for, or ensuring the ways in which the data is subsequently used are consistent with consents provided or any other legal grounds to support the activities.

Data Storage

45%

take data storage risks into account only when considering strategic projects.

Data Clasification

45%

of organisations do not distinguish between different types of 'sensitivity' of personal data, instead treating all types of data in the same way.

Right to access, rectification, deletion and objection

15%

of organisations have procedures in place which would enable them to easily respond to requests by individuals for access to copies of their data files.

Data Retention Policies

15%

have a comprehensive data retention policy which is applied across the organisation.

Data Security Breaches

20%

of organisations have fully implemented data breach incident response procedure.

¼

of these organisations regularly prepare for a data breach by conducting desktop exercises.

Data Protection Officer

30%

of organisations have a full-time data protection officer.

FINANCIAL SERVICES

Many financial services institutions still require a great deal of work to determine their approach to prepare for GDPR. The responses to the Scorebox indicate that the current level of maturity among financial institutions for central data record keeping and accountability requirements of the GDPR are low, reflecting the more limited record keeping requirements and benign nature of the current regime. A much more thorough analysis of personal data collection and use and documenting exercise will be required under GDPR.

GDPR also creates significant additional risk and exposure in the supply chain. All supply chain contracts where suppliers are processing personal data on behalf of institutions (either as processor or, in more limited scenarios as joint controllers) will require an extensive re-papering exercise prior to May 2018 if they are to meet the requirements of the GDPR.

FINANCIAL SERVICES

Privacy Policies

47%

of organisations have privacy policies in place for all business functions which routinely process personal data.

Specifying the use of personal data

33%

of organisations always ensure they have a detailed view of the purpose for which personal data is collected, in advance of collection.

Maintaining accurate data records

19%

do not routinely check records are accurate and up-to-date.

50%

update records on an ad hoc basis if they are made aware of inaccurate data.

19%

of organisations have robust processes in place to ensure records remain accurate.

11%

of organisations do not know whether their records remain up-to-date.

Data Protection Officer

36%

of organisations have a full-time data protection officer.

Internal standards and procedures

50%

have fully implemented internal standards, procedures and guidelines to assist employees in the collection, use and sharing of personal data.

⅓ of these regularly audit these standards and procedures.

Cross-border transfers and sharing of personal data

77%

of organisations make cross-border transfers.

64%

are confident that these transfers are managed in line with relevant rules.

Notifications and Approvals

47%

of organisations have up-to-date notifications and approvals required by the relevant data protection authorities in each of the countries where they operate.

Security Policies

69%

of organisations have fully implemented information security policies.

Data Security Breaches

44%

of organisations have a fully implemented data breach incident response procedures.

⅓ of these organisations regularly prepare for a data breach by conducting desktop exercises.

TECHNOLOGY

The technology sector was one of the highest responding sectors, but the responses indicate that only a third have a high level of maturity in their engagement with the GDPR legislation. That is surprising in a sector where data processing is a core activity.

There are two major GDPR risk areas for the technology sector. Firstly, the rise of cloud technology, which means that many technology companies are routinely processing personal data on behalf of other companies. In this context, technology providers have a very important responsibility and considerable penalties will ensue if the data is mishandled or inadequately protected.

Secondly, and linked to this, the new legislation introduces the principle of 'Privacy by Design', which requires that data privacy requirements should be considered at all stages in the development of new products and services.

TECHNOLOGY

Updating Privacy Policies

For organisations with Privacy Policies in place:

25%

of organisations have static privacy policies.

52%

of organisations update their privacy policies on an ad hoc basis.

23%

of organisations regularly update their privacy policies, on an annual basis as a minimum.

Storage of data

25%

of organisations decide on how and where to store data based on commercial factors such as pricing, as opposed to data protection risks.

Intra-group data sharing

18%

of organisations maintain a register which clearly shows data sharing principles and authorisation to process data by each group company.

Data Protection Officer

20%

of technology organisations have a full-time data protection officer.

Employee Training

50%

do not conduct employee training.

23%

have employee training on an incidental basis and it is not compulsory to attend.

21%

make their employees attend at least one training session.

10%

make their employees attend an initial training session, followed by refresher training.

Security Classification

40%

of organisations apply a single set of security standards to all data types.

Data Security Breaches

33%

of organisations have a fully implemented data breach incident response procedures.

1/3

of these organisations regularly prepare for a data breach by conducting desktop exercises.

ABOUT THE REPORT & METHODOLOGY

DLA Piper's Data Privacy Scorebox

The data in this report was collected via DLA Piper's Data Privacy Scorebox.The Data Privacy Scorebox is an online survey designed to assist organisations with assessing and benchmarking their data privacy maturity level.

It is a complimentary survey which poses a series of questions relating to 12 areas of data privacy, such as privacy policies, the use of data, security measures and individuals' rights. Respondents gave their answers by selecting the most relevant statement from a range of multiple choice answers.

If you would like to assess your organisation, please visit www.dlapiper.com/dataprotection to access the Data Privacy Scorebox.You will receive a dashboard summary of your organisation's alignment with 12 key areas of global data privacy, as well as a practical action point checklist.

Snapshot of Data Protection Maturity

The Data Privacy Scorebox was launched on International Data Protection Day in January 2016, and in the year since then, over 250 organisations from 13 different sectors have completed the online survey. We have analysed this data and produced this report as a snapshot of the Life Sciences and Healthcare, Financial Services, and Technology and Telecoms sectors.

DLA Piper's Data Protection, Privacy & Security Practice

The Data Privacy Scorebox has been created by members of DLA Piper's Data Protection, Privacy and Security group.The 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 100 multinational organisations in the design and implementation of global privacy and security programs.

For further information please contact us by email at:

dataprivacy@dlapiper.com

Data Protection, Privacy & Security Tools

Our global team has developed a range of complimentary tools to assist organisations with data protection, privacy and security matters.These include a dedicated European Data Protection Regulation microsite, our highly regarded Data Protection Laws of the World guide, and a security breach response guide.

Find out more:

www.dlapiper.com/dataprotection

DLA PIPER