Data Privacy Laws: Cutting the Red Tape

an Ovum report commissioned by Intralinks

Contents

Executive summary

A global privacy rights movement poses significant new business and economic risks

National governments are enacting new, stringent data privacy laws to protect citizen data, guard national security interests, and potentially provide a boost to local industries. This rush to protect sensitive and personally identifiable information threatens current business strategies, practices, and processes widely used by organizations that operate internationally.

To explore the impact of evolving data privacy regulations and data sovereignty, Ovum was commissioned in Q3 2015 by Intralinks to conduct an international survey of 366 IT decision-makers.

Key findings include:

Data privacy regulations are coming directly into conflict with cloud, software-as-a-service (SaaS), and mobile computing practices within enterprises

Cloud computing is an established part of the enterprise IT landscape, and adoption is expected to continue to increase over the next decade. Information-intensive business processes rely on SaaS, and this, coupled with a shift to mobile computing platforms, means controlling data location and complying with privacy regulations is extremely challenging. Nevertheless, over the next three years, 78% of survey respondents plan to use cloud and SaaS-based applications, even for storing and sharing sensitive and regulated data

Business leaders are deeply pessimistic about the potential consequences of new data privacy regulations

Our survey shows that organizations are aware of data privacy as an issue but are struggling with how to respond. When we asked about the pending European Union (EU) General Data Protection Regulation (GDPR), 52% said they think it will result in business fines for their company, and two-thirds expect it to force changes in their European business strategy.

The cost of regulatory compliance will be substantial, but the cost of non-compliance will be higher

Over 70% of respondents expect to increase spending in order to meet data sovereignty requirements, and over 30% expect budgets to rise by more than 10% over the next two years. Of those who plan to update data privacy strategies in the next three years, 38% plan to hire subject matter experts, and 27% will hire a chief privacy officer.

US-based organizations are particularly vulnerable

The Snowden Effect is real. Among 20 industrialized economies, the US is ranked as the least trusted country and the most likely to gain unauthorized access to sensitive information with China coming in second and Russia third. New regulations will also put US companies at an even greater disadvantage, with 63% of respondents believing that the proposed EU GDPR regulations will make it harder for US companies to compete, and 70% thinking the new legislation will favor European-based businesses.

Most organizations aren't effectively using technology to address data privacy concerns

Alarmingly, many organizations aren't taking advantage of available technologies that protect sensitive data. Only 44% of survey respondents monitor user activities and provide alerts to data policy violations, and only 53% classify information to align with access controls. Almost half (47%) have no policies or controls that govern access to consumer cloud storage and file-sharing systems like Dropbox.

Global organizations need an orchestrated approach to data sovereignty that covers people, process, and technology

Business leaders recognize the need to take a balanced approach to address data sovereignty and data privacy. When asked about investment strategies, 55% said they are planning new training for employees, 51% will amend and adapt policies, and 53% will prepare by adopting new technologies.

Organizations face a patchwork of contradictory and conflicting global privacy regulations, and need technology options to address all eventualities

The data sovereignty revolution threatens to create a Balkanized technology landscape, with different jurisdictions imposing inconsistent and often incompatible mandates for how personally identifiable data is stored, processed, and shared. This is already creating confusion and uncertainty, leaving fundamental questions unanswered, such as how to interpret data location requirements. Organizations need technology options that enable them to react to a rapidly changing regulatory environment.

Introduction

Even before Edward Snowden's revelations showed the full extent of the US National Security Agency's (NSA) electronic surveillance, data privacy was becoming a global issue. Government snooping combined with massive data leaks over the last few years have forced national governments to recognize that current privacy laws have outlived the paper-based age and need to catch up to the realities of the digital economy. The result has been an unprecedented wave of new legislation designed to govern how certain sensitive data can be gathered, stored, processed, and shared.

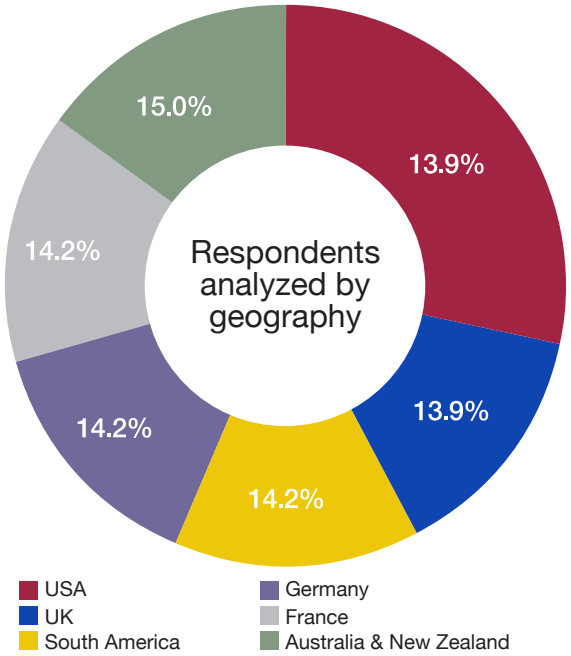
Countries as diverse as Brazil, Singapore, and Russia are tightening regulations. The EU is nearing the end of a lengthy process of revising legislation in this field, which will affect any organization operating in its member countries. These restrictions are being imposed because organizations are becoming borderless and employees more mobile, which along with a migration to cloud-based IT systems can cause conflict with these new laws. The compliance obligations arising from legislation are becoming more complex, particularly for organizations that operate across different jurisdictions, and particularly in the context of how legislation applies to data that is stored by cloud-based services.

In Q3 2015, Ovum was commissioned by Intralinks, a leading provider of enterprise cloud content collaboration solutions, to understand the implications of data privacy regulations on global businesses.
A survey was conducted to explore the following questions:

- How are organizations preparing to deal with data sovereignty?
- What will be the impact of new data privacy regulations?
- How will organizations adapt their business to meet new privacy obligations?
- What are the differences of opinion in different countries and in different jurisdictions?
- What technology decisions will support data privacy obligations?
- What are the best practices for adapting to new regulatory regimes?

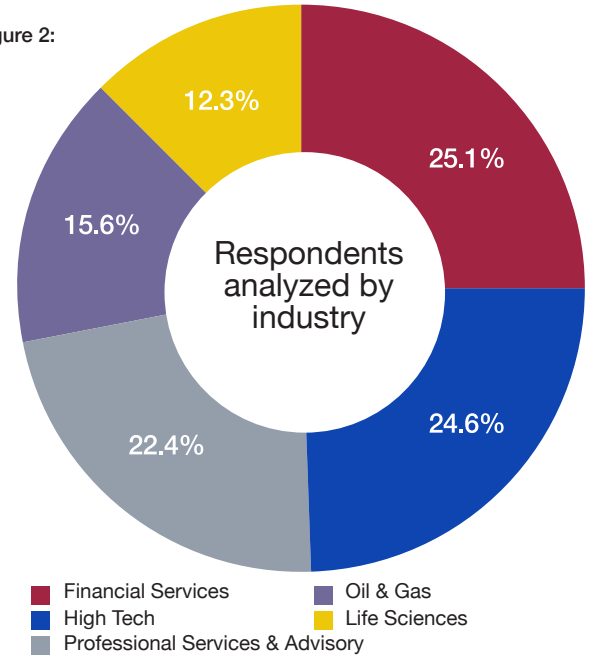
Ovum's survey incorporates input from 366 respondents from across the globe, within organizations of different sizes, in various industries (see Figures 1, 2, and 3). The demographics were chosen deliberately to include a variety of organization types and countries being affected by data privacy regulations and data sovereignty obligations.

Figure 1:



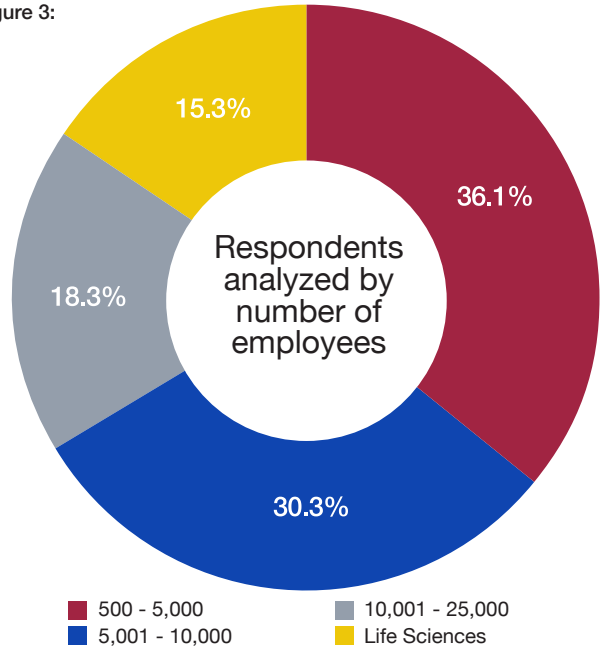
Source: Ovum

Figure 2:



Source: Ovum

Figure 3:



Source: Ovum

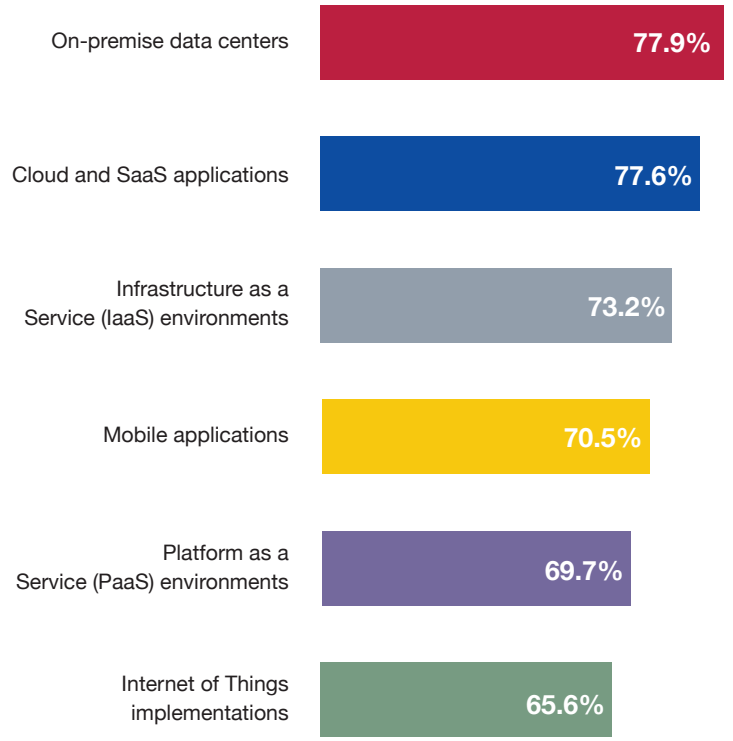
Enterprises face major compliance challenges

Continuing cloud usage is inevitable

Cloud computing fuels productivity in modern business. It connects the entire workforce, bridges relationships between organizations, business partners, and customers, and connects us all socially. It has transformed how we communicate and deal with information, radically changing the world's most established companies and how IT budgets are managed. For example, recent Ovum research found that one-sixth of organizations' overall IT budgets is already typically spent on SaaS, and that spend on cloud-based solutions is expected to grow. About four-fifths of enterprises are now using or planning to use cloud computing across deployment (private, public, and hybrid) and service (IaaS, PaaS, and SaaS) models, up from two-thirds at the start of 2014. The market is expanding as new generations of adopters come to the fore. The second wave of adoption has reached full momentum, and a third wave, of latecomers, has also started to swell in 2015.

The data sovereignty survey provides new evidence on how much the cloud is trusted to house regulated and sensitive data. This is in stark contrast to a few years ago, when conversations revolved around whether the cloud should be trusted at all. Now, it is trusted to protect the most sensitive assets (see Figure 4), demonstrating a shift in sentiment toward its positive role in business today. The survey also found that 58% of respondents trust the cloud for all business operations, despite the potential impact of pending data privacy regulations, all of which intend to change how data is stored, transferred, and processed around the world. So, even with the changing regulatory climate, cloud computing is a decision that's already been made. And yet, regulating cloud-held data is fast becoming the biggest problem facing legal practitioners, politicians, and businesses as they try to balance privacy with access and productivity.

Figure 4: Responses to "In which of these tech environments is your regulated and sensitive data going to be present within the next three years (i.e. by mid-2018)?"



Source: Ovum

Ovum believes that part of the reason for favoring cloud computing is a resourcing issue. It is no secret that organizations often have limited resources to apply the right protection to regulated and sensitive data or to prove adequate compliance if the data is held internally. As such, data protection itself is becoming another driver for cloud adoption because customers see cloud providers as likely to "wrap" the best security arrangements they can as part of the service package.

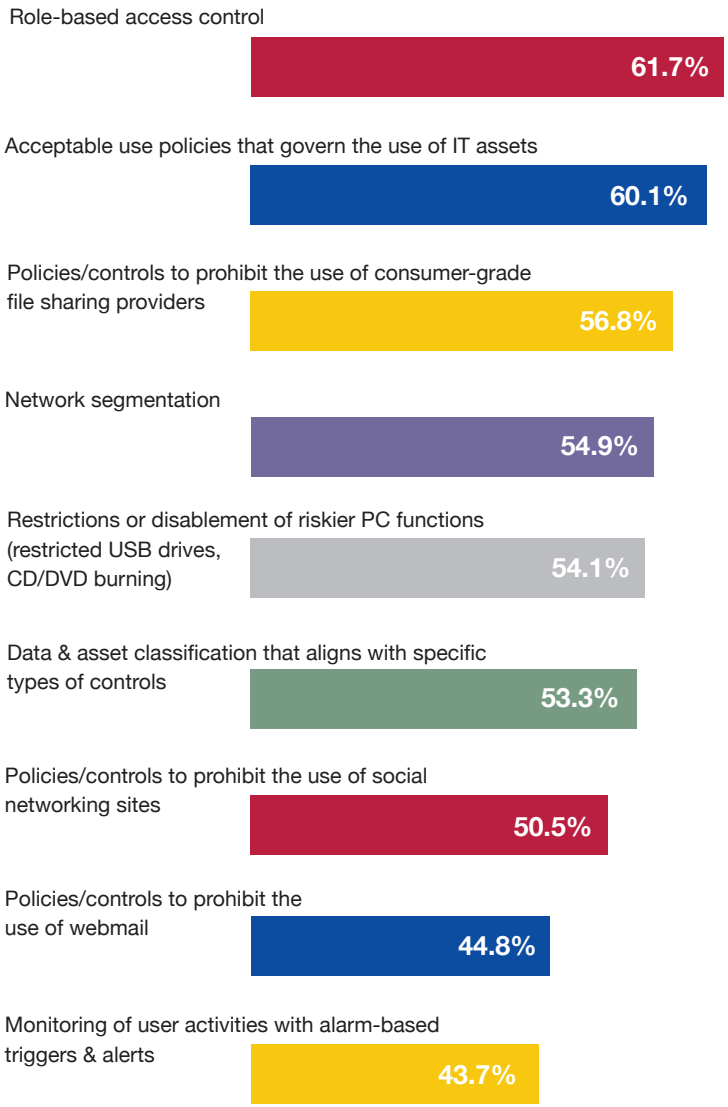
Organizations aren't taking basic steps to protect sensitive data

We also found that many respondents are not even applying basic measures to protect data and meet current compliance requirements (see Figure 5). Only 44% of respondents monitor user activity and have policy-based triggers and alerts, and only 62% have adopted role-based access controls. Just over half (53%) actually classify information assets to facilitate controls. We found that even rudimentary measures aren't being taken, and only 54% disable PC features such as external attached drives, and only 57% block access to ungoverned consumer storage and file-sharing apps such as Dropbox.

It's likely that organizations with these gaps in data protection will look to cloud providers for help instead of spending time and resources trying to fix data issues internally. Further analysis of the survey results shows that the general shortfall in data privacy measures applies particularly to smaller and midsize organizations. It is likely that, for them, upgrading data protection capabilities will require a proportionally higher investment, explaining this result.

Customer focus from all types of organizations on the precise scope of this protection is likely to increase as they become aware of greater compliance responsibilities to provide adequate safeguards for sensitive data, and the relevant technologies to do so is in the hands of cloud and SaaS providers.

Figure 5: Responses to "What policies, processes and controls does your organization currently deploy to help protect data and avoid misuse?"



Source: Ovum

Data privacy regulations aren't uniform, leaving global businesses vulnerable and confused

Where organizations are already failing to implement standard data protection measures, new, stricter data privacy laws will leave them even more adrift. Data privacy laws are being written locally, without any overall governing framework to impose order. Global organizations operating across multiple jurisdictions are faced with a patchwork of laws that demand different responses (see Table 1). It's also not clear exactly how current laws may change. For example, Safe Harbor, a 15-year-old data transfer agreement between the EU and the US, was recently declared invalid, affecting over 4,000 businesses that can no longer legally transfer data outside of the EU to the US without the cover of other legal devices such as model clauses, or binding corporate rules. This leaves global businesses, especially those with a presence in Europe, confused about the safest course of action, and concerned that they are now in violation of the law.

Table 1: Current status of data protection regulation

Country/ region	Definition of personal data	Forms of consent required for personal data treatment	Rules for the transfer of personal data abroad	Requests for data from public bodies	Penalties
EU	Information relating to an identified or identifiable natural person. Draft regulation includes IP addresses.	"Unambiguous consent." Draft regulation aims to introduce explicit consent.	The EC and member states decide whether a third country provides adequate protection; if not, safeguards have to be in place.	Unclear after the repeal of the Data Retention Directive. National laws still formally in place.	Sanctions are decided at country level. Draft regulation proposes fines up to 2% of a company's annual turnover.
US	Unclear. Varies across different acts/ industries.	Prior "written or electronic consent" in the Communications Act.	No specific rules. The Federal Trade Commission (FTC) maintains that US law still applies when data leaves the US.	A court order is generally required. The FBI and other agencies have exceptions under Patriot Act.	Sanctions vary across different acts.
Australia	"Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable."	Organizations must take "steps as are reasonable in the circumstances" to notify an individual about that collection.	Transferring organizations must take reasonable steps to ensure that the principles of the act are not breached once data is sent to another country.	A government agency must not collect personal information unless said information is reasonably necessary for, or directly related to, one or more of its functions or activities.	Civil penalties of up to $1.57m (A$1.7m) for serious or repeated breaches of the act.
Singapore	"Data, whether true or not, about an individual who can be identified either from that data or together with other data or information to which the organization is likely to have access."	Consent should be obtained in writing or recorded in a way that can be stored for future reference, although it may be gained verbally.	Transfers are permitted if the same level of data protection is afforded in the receiving country.	Public agencies and organizations acting on behalf of a public agency are exempted from the Personal Data Protection Act (PDPA).	Financial penalty of an amount not exceeding $799,000 (A$1m).
Brazil	Unclear. The "Internet Civil Framework" will be completed by more detailed regulation.	"Free, informed, and explicit consent." Upcoming regulation may define this more in detail.	Transfer is permitted, but companies have to comply with Brazilian legislation if any data collection/ processing takes place in Brazil.	Retention time is one year for ISPs' connection registries, and six months for application providers. Police or courts may require an extension.	Up to 10% of the turnover of the company in Brazil, excluding taxes, and temporary or complete suspension of data collection and processing activities.

Source: Ovum, and quoted verbatim text from legislation

Pending European regulations will set the standard for global data privacy, but will jeopardize the EU economy

Measured by GDP, the EU as a whole is the largest economy globally, according to the International Monetary Fund (IMF) and the World Bank. It therefore has the ability to set the regulatory standard for other global regions, and any European legislation will unavoidably impact all organizations that operate internationally. Provision for the protection of data privacy within the EU was first made under the Data Protection Directive of 1995. However, a few years ago there was widespread recognition within the EU authorities that technology had moved on, and a new regulatory regime (the pending GDPR) would be required to deal with the business adoption of smartphones, tablets, universal broadband connectivity, and cloud services. Table 2 provides a summary of some of the major changes in the GDPR.

Our survey has revealed that global companies intend to change business operations in some European countries once the GDPR is finalized. According to our sample, 78% of US companies, 62% of UK companies, 58% of French companies, and 71% of companies in companies, 46% of South American companies, 71% of German, Australia, and New Zealand (ANZ) all intend to review their approaches. This could mean a serious economic blow to the EU, the prosperity of which relies on international business. Underpinning this decision is cost, with 68% of the global respondents believing that the GDPR will dramatically increase the costs of doing business in the EU. Also, 85% of US companies believe that it will be harder to compete against European companies, which could mean the number of US companies operating in the EU will decrease. These results demonstrate huge uncertainty around the GDPR, with companies foreseeing a negative impact on global business and probably the EU economy as a result.

Another concern raised by our respondents is potential penalties. The extent of fines to businesses in the event of a GDPR violation is potentially 2% of global revenue, which means billions of dollars for the world's highest-profile companies. According to our research, over 50% of global businesses believe they will be fined as a result of the GDPR. If we break this down by country and region, it means that 62% of German companies, 59% of US companies, 53% of UK companies, 42% of French companies, 56% of ANZ companies, and 32% of South American companies think they will be fined as a result of the GDPR.

Table 2: Some of the major changes in the GDPR

GDPR issue	Change	Impact
One-stop shop	Companies will agree their compliance stance with a single EU-wide regulator instead of one per member state	Simplification of compliance. NB this plan is still not 100% guaranteed to come into force
Data processors	Data privacy legislation is extended from data controllers and subject to a new class of actor, the data processor	Cloud service providers, SaaS providers et al need to comply with EU Data Privacy law
Extraterritoriality	Companies headquartered outside the EU are covered by the law if they are handling data on EU residents	Non-EU service providers may need to invest in local data centers, as one approach
Data residency	Data on EU data subjects cannot be transferred outside the EEA without legal cover. (See information outside this table about the demise of cover under Safe Harbor certification)	As above
Profiling	A data subject will need to give consent for their data to be passed to other data controllers than the one to whom they gave it for purposes of profiling	This will potentially impact data processors if they are using or forwarding information to other data controllers, or indeed using it themselves for profiling purposes. NB there is still debate as to whether consent will need be explicit or can be implicit

Source: Ovum

Overall, most global companies (57%) believe the GDPR is an over-reaction to the surveillance practices revealed by the material Edward Snowden released. Oddly, European respondents also agree with this sentiment, with 57% of German respondents, 51% of UK respondents, and 46% of French respondents saying the GDPR is an over-reaction to the problem of data privacy rights. Again, the motivation behind these responses is likely to be the cost implications from the perspective of both fines and business strategy.

Data location is the critical point of control but is hard to define

From a legislative viewpoint, the matter of "where data is" is critical. In the debate about data sovereignty, fundamental concerns include data location and the clear definition of the point of control over personally identifiable data. In our research, there is uncertainty and confusion about these seemingly obvious concepts. The ability to exert sovereignty over corporate data (to control access to the data) and achieve compliance is heavily dependent on the data's location, because its location is a factor in determining what legislation the data is affected by, and the level of access that should be available. Exerting control over data location is a considerable difficulty for many organizations, because most systems do not support the concept of data location being a business-related decision, and especially not cloud-based systems. The complexity around this issue is worsened because the exact definition of data location for compliance purposes varies across different items of legislation, and can be open to legal interpretation in places. Organizations trying to achieve compliance may well need options that offer control over data's physical, logical, legal, and political location. Indeed, we are already seeing legal arguments being made in courts around the world that hinge on the fundamental concept of where data is located and controlled, and who has jurisdiction over that data (an example is the Microsoft case regarding data stored in Dublin, Ireland that is being requested by a US judge).

Our survey shows (see Table 3) that there is no clear consensus on these questions of data location. We also found that 50% of respondents' organizations planned to change the primary approach to this control during the next three years. This may reflect uncertainty over the capacity of our respondents' current approach to cater for new requirements, and also over which approach they should choose. It may also suggest that organizations are waiting for a standard to emerge. It argues strongly for an approach that provides various technical options, such as the ability to offer controls for physical and logical location.

Table 3: Respondents' current / possible approaches to tackling data privacy

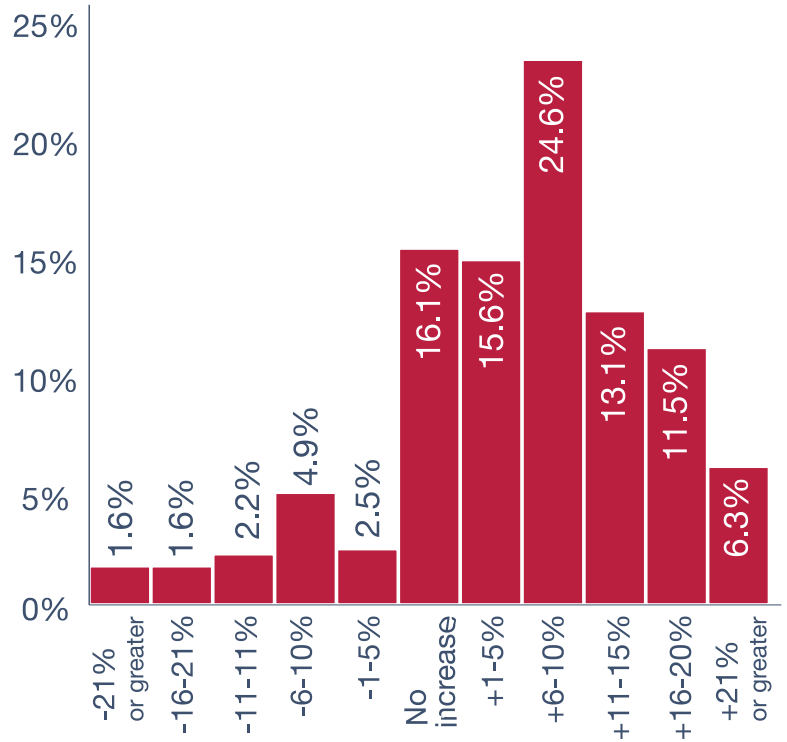
Answer	Current primary approach	Considering this approach
We make our data privacy decisions using the legal location of data (This refers to country or countries that are likely to have jurisdiction over the data – and the jurisdiction whose laws must be broken for someone to access the data against your will.) – e.g. a country responsible for its own laws governing these matters	26%	27%
We make our data privacy decisions using the logical location of data: (The geographical location from where control is exerted over a given computing function, i.e. where the point of encryption resides.)	27%	33%
We make our data privacy decisions using the physical location of data: (Traditionally, the geographic location(s) where the information is actually written to storage.)	33%	24%
We make our data privacy decisions using the political location of data (This is the likely point of application of governmental pressure to release content.) – e.g. the US, or EU	14%	15%

Source: Ovum

Regulations impose huge costs

As the regulatory climate changes (as in Hong Kong, Singapore, and Russia, for example), budgets are being affected. Data privacy regulation is traditionally a legal problem, but because it will now impact the technology and compliance functions, our research shows that a great many companies are expecting to make recruitments in these departments to tackle the implications of pending data privacy regulations. When broken down, 19% expect hires in the legal function, 31% expect hires in the technology function, and 34% expect hires in the compliance function. In turn, this raises more questions about changing job roles and the legal, compliance, and technology skills that will be most valuable as new regulations come into full force.

Figure 6: Responses to "What budget alterations do you expect in the next two years as a result of global regulatory reform related to data protection/data sovereignty?"



Source: Ovum

According to our results, the respondents believe that technology and compliance professionals are the most appropriate hires to support what is usually defined as a legal problem, and it is likely that we will see more technology and compliance specialists learning more about data privacy law in the next few years.

Clearly, with such a scope of impact, costs will mount. Our survey indicates the expected effect on overall budget (see Figure 6). It is notable that over 30% of respondents expect budgets to increase by at least 10%, and almost a quarter expect between 6% and 10%. Overall, more than 70% of respondents expect their budgets to increase due to pending data privacy regulation.

US-based organizations are under pressure

As a consequence of Edward Snowden's revelations about the surveillance activities of the US National Security Agency, the US faces a lot of distrust. We asked respondents to rank major industrialized countries based on which they believed would access their data without permission, and the US was considered the least trusted, with China and Russia in second and third places respectively. In reality, legal due process in the US provides strong privacy protection, arguably better than even some European countries, but opinions have been heavily influenced by the media storm that gathered pace after the revelations. New regulations in Europe will also put US companies at a disadvantage. In our survey, 63% of respondents believe that the proposed EU GDPR regulations will make it harder for US companies to compete, and 70% think the new legislation will favor European-based businesses.

Recommendations

Data sovereignty issues arising from legislation are going to have a major impact on very large numbers of organizations that have international operational scope. Organizations need to balance business, legal, and consumer requirements as they handle personally identifiable information. Actions needed now include:

Establish a data sovereignty strategy

Companies that operate internationally and which gather personally identifiable information (PII) are subject to data privacy regulations in all of the countries in which they do business. Organizations are not protected from responsibility because they rely on a third-party cloud provider to manage data. The first step is to recognize this responsibility and create a strategy to react. This strategy should be managed by a core executive team, responsible for establishing corporate controls, policies, and procedures for maintaining compliance. Your GRC team may have already embarked on this process, but your executive team needs to be a sponsor.

Conduct a privacy risk assessment

Good governance must incorporate identifying significant risks to the organization. Context is extremely important when assessing privacy exposure, and certain industries such as life sciences companies and insurance providers face significant regulatory oversight and scrutiny. The privacy risk assessment should begin by classifying information into broad categories (PII, company confidential information, for example) and mapping this to existing business processes and related geographies. Identify and review pertinent privacy regulations in each jurisdiction in which you operate. Be prepared to change business processes to meet regulatory demands. You may already have technologies that can help with your content assessment (for example, data classification tools such as Atlas) and, conversely, you are likely to have technologies in use that increase your risk (for example, consumer file-sharing tools such as Dropbox).

Include people

Legal and technology issues within the scope of assessing the effects of data sovereignty issues: Acknowledge that data privacy and data sovereignty are complex challenges that touch your entire business. Educating your workforce is as critical as implementing technology solutions to manage data flows. It is not financially viable or legally sound to just focus on technology, process, or employee activity individually because all three are important.

Start discussions now

With existing technology and service providers about their plans to cater for new legislative requirements: Savvy vendors are already prepared to provide options for addressing data privacy concerns. Optionality is critical because laws will be inconsistent form country to country and are changing rapidly. Vendors should be able to answers questions about logical and physical data location, and have service contracts that also give legal flexibility.

Appendix

Methodology

Ovum's survey, conducted in Q315, incorporates 366 responses from organizations of different sizes, in different global areas, across a range of industries. Analysis of the survey results has been undertaken in the context of ongoing consultations with Ovum clients, discussions with industry vendors, and secondary research.

Author

Alan Rodger, Senior Analyst, Enterprise ICT Management
alan.rodger@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you.

For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

CONTACT US

www.ovum.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo