druva

White Paper

Preparing for The New World of Data Privacy: What Global Enterprises Need to Know

This paper is for senior IT leaders who are addressing data privacy concerns in their organizations

Executive Summary

There is increasing global consciousness about data privacy today due to strengthening data privacy regulations around the world. News regarding the NSA's mass electronic surveillance data mining program (PRISM), large-scale surveillance practices by EU member states, highly publicized data leaks and thefts, and bring-your-own-device (BYOD) policies are bringing heightened awareness to this issue. Global corporations know they must adapt their IT infrastructure to support increasingly varied regional data protection regulations or face potential sanctions and/or legal repercussions, but not everyone knows exactly what is needed to operate in the new data privacy landscape. This paper sets forth recommendations for enterprises preparing for this new world of data privacy compliance.

Business concerns about storing data in the cloud

There has been a significant shift in enterprise IT to the cloud, given recent improvements in cost efficiency and growing confidence in cloud security. According to the consulting firm BCG, software as a service (SaaS) is growing at three times the rate of on-premises software.[1] This is happening because there are several benefits to cloud computing. Businesses can shift their capital expenditures to operating expenses, leaving them with more money to put toward core projects. Projecting expenses becomes much easier with a subscription model. And, cloud services also save IT resources and provide a shorter time to value because there's no software to install or equipment to manage.

A large majority of businesses are using the cloud for email and productivity applications, and to store accounting and financial information, payroll data, patient billing information, administration information, medical records, and intellectual property. IT teams, as traditional custodians of corporate data, are challenged with not only preventing the exposure of this data, but also backing up and protecting the organization's intellectual property in case a device is lost or stolen, an employee leaves the company, or for eDiscovery in the case of litigation.

Organizations see tremendous cost, flexibility, and scalability advantages in backing up data on laptops, mobile phones and other endpoint data to the cloud, but they have several concerns around trusting their data with a cloud service provider, particularly with regards to privacy, security, and availability of sensitive data across myriad devices and network connections. Depending on the industry or the geographical location of an organization, it could be subjected to various regulations, such as HIPAA or data residency laws, and the business must then ensure that it remains compliant with all of these regulations, even if its data is stored in the cloud. Businesses also want to ensure that end user productivity is not impacted by downtime of the cloud service, and that they don't risk permanent data loss when trusting a third party with their sensitive corporate data.

1. Profiting from the Cloud: How to Master Software as a Service

Meeting the needs of data residency compliance

Many countries have implemented regulations to legally protect corporate data, including personally identifiable information (PII), private health information (PHI), personal and corporate tax information, corporate financial information, and telecommunication information. Violation of these regulations can result in fines and criminal prosecution of the individuals responsible for data exposures. The rise of cloud data storage and backup is causing IT leaders who deal with data privacy and security to figure out ways to minimize legal and regulatory liabilities while meeting their operational data storage requirements.[2]

Depending on their location, businesses could be subject to data residency laws and regulations, where they can only have their data in a certain geographical region. Global organizations that have employees across different countries require access to data centers in multiple regions, closer to their users. Cloud providers should be able to leverage regional data centers around the world, so they can address regional variations in privacy rules and meet the needs of the global enterprise.

For example, some providers have their data centers in Europe, but the US has access to the data or metadata stored there, which is a significant concern for companies doing business in countries with strict regional data residency regulations. Microsoft has been dealing with this very issue in court lately. In December 2013, US federal prosecutors requested a search warrant to obtain the contents and metadata of a Microsoft user account, in relation to a drug investigation. While the metadata was stored in the US, the contents of the emails were stored in Ireland. Microsoft refused to turn over the emails, stating that the US government does not have jurisdiction to force a company to produce data stored in another country. According to InformationWeek, "Microsoft is arguing for the right to retain access to data stored on its servers without providing that data on demand. A loss could mean that the only viable option for cloud computing companies is to adopt a zero-knowledge policy — to be unable to unlock customer data in the cloud, a stance Apple and Google have already taken for data on mobile phones."[3]

The European Union's Data Protection Act (DPA) differentiates between "data controllers" — individuals or entities that determine the purposes for and manner in which any personal data is to be processed — and "data processors" — individuals or entities that process the data on behalf of the data controller.[4] The essential difference between the two is that one has the authority to process information, and the other can decide who can process the data. This wall of separation allows organizations and governing bodies to be able to determine responsibility in the event of a data breach.[5]

Following this model, some cloud vendors offer different levels of administrator access, depending on the admin's department and individual role. At one level, administrators have overall admin rights across all areas of service, and can revoke access of other admins at any time. At another level, administrators have rights limited to user profiles or regionally segregated administrative rights. These delegated administrative capabilities enable organizations to uniquely

2. Five Cloud Data Residency Issues That Must Not Be Ignored
3. Microsoft Gains Allies Against US Data Demands
4. Information Commissioner's Office Guide to Data Protection
5. Data controllers and data processors: what the difference is and where the governance implications lie

configure privacy settings, while still providing a single system of record managed by the enterprise.

Why it's important to address privacy — not just security

Much of the data privacy debate takes place in the context of network security and defending against outside threats. When one thinks about data being compromised, it's usually in the context of a cyber security attack by a malicious external entity who figures out how to hack into systems and steal data, which leads to confusion about security versus privacy. While it's certainly important to defend against cyber attacks, it's equally important to understand how much sensitive information is flowing relatively freely inside organizations, without proper controls in place to avoid corporate and employee data mishandling and misuse.

"Securing data is important, but addressing security without enacting appropriate privacy measures leaves data — and companies — vulnerable. Today, more than ever, global organizations must comply with regional data regulations," says Jaspreet Singh, CEO at Druva. "Privacy concerns are being forced into IT's top priorities. Focusing exclusively on security can compromise privacy, exposing organizations to negative publicity as well as possible legal and regulatory action."[6]

Data privacy is a multi-pronged issue. It begins with how data is stored and secured, but also includes processes and controls to address broader privacy concerns. Cloud vendors typically address data privacy and security by providing authentication and access controls. This ensures that only the right people have access to corporate data. Encryption keeps the data secure, but it doesn't necessarily guarantee that the data is private. What really matters is where the encryption keys are stored and who has access to them. If a cloud service provider has access to a company's encryption keys, either directly or through an escrow provider, then it can provide access to that company's data. And if the provider is ever subpoenaed, it can provide that data without getting the customer's permission. In these models there can be a high level of security, but the data is not truly being held private.

Sometimes encryption keys are stored on the server behind the corporate firewall. While this prevents the service provider from accessing the keys, it requires additional management of hardware or a key server on premise, which negates the reason for selecting a cloud service and creates a single point of failure to accessing your data.

With today's mobile workforce, users want to be able to access their data anytime, anywhere. This means they need the ability to self-restore their data if something were to happen. In most implementations, users can only self-restore if the end user device holds the encryption key. But storing the key on the device can create additional security risks. If the device storing the key is lost or stolen, and the device itself is not encrypted, the key can be accessed by an outsider.

The business case for better systems to support data privacy

As more and more data moves to the cloud, and consumer applications are being adopted by the workforce, new privacy concerns are appearing within organizations. Sensitive financial data, PII, and other data are making their way onto devices and networks outside the view of IT. Despite this fragmentation and lack of visibility, under the terms of data privacy regulations, organizations are morally and legally required to protect the privacy of their users' data. While many organizations have the foresight to put policies and procedures in place to ensure data security and privacy, it does not mean that these are followed. Putting that responsibility in the hands of individuals and expecting them to strictly follow those guidelines is unrealistic. Technology like encryption, data segregation, and policy setting

6. Druva Announces Cloud Data Privacy Framework

can fill in the gaps to help companies enforce regulations and maintain compliance with data privacy policies. When developing privacy guidelines, it's important for businesses to consider how systems support data privacy through different capabilities within the products they're using.

According to Rick Kam, president and cofounder of ID Experts, businesses should take a proactive stance, viewing data privacy as part of their day-to-day organization, rather than waiting for a data exposure incident. "As new risks come into place, like BYOD, cloud computing, information exchanged through health exchanges and so forth, policies, procedures and technologies need to be addressing these risks," says Kam. "So besides employing standard risk management practices like annual risk assessments and point-in-time risk assessments for new applications, these new risks really need to be addressed in a holistic fashion."[7]

Businesses recognize that users are getting more productive by making use of BYOD and file sharing solutions. While IT is focused on protecting and securing data, and having visibility into stored data, employees are worried about convenience, productivity, and privacy of their personal data. To address these concerns, organizations need an IT-managed way to avoid accessing employees' personal data that may reside on devices alongside corporate data. Employees in companies with BYOD policies have the right to use their devices for both personal and corporate data. The employer has access to all of the data on those devices, but needs to be conscious of not copying or viewing the employees' personal data to ensure that privacy remains intact; this is especially at issue at the global level.

How Druva inSync maintains data privacy in the cloud

Companies are realizing that they need to rely on solutions designed specifically for the purpose of maintaining the privacy and security of corporate data, that security itself will not meet today's global requirements. Endpoint backup, data loss prevention, file sharing, and data governance tools can comprehensively protect corporate data by adhering to strict standards ensuring data privacy and security in the cloud.

Druva inSync centralizes and controls business data residing on employees' desktops, laptops, tablets, and smartphones via integrated backup, data loss prevention, IT-managed file sharing, and data governance controls. inSync continually mirrors employee device data, creating a centralized, monitorable repository of enterprise information. This enables data recovery for lost or stolen devices, allows remote user access to any file or folder from any device, and supports eDiscovery, compliance, and forensics needs.

inSync has a combination of safeguards in place for protecting organizations from unauthorized access, preventing misuse of employee data by authorized users, and ensuring data integrity regarding legal or compliance initiatives. Regional storage provides support for 11 global admin-selectable regions that are policy-configurable to ensure data is stored to meet DPA requirements. Single instance object storage of block data keeps data separate from metadata, delivering data scrambling with no ability to cross-reference stored objects. Metadata and blocks are both encrypted using a unique envelope key encryption model that ensures data privacy; nobody — not even Druva under court order — can provide access to customer data. End-user privacy controls can be set to private, depending on regional requirements, to ensure administrators cannot have visibility into their data.

A privacy policy for officers who may be handling sensitive materials prevents them from having their data seen by anyone else in the organization. Audit trails for end users and administrators ensure that all data access and file sharing activity is tracked with tamper-proof audit logs, so that data privacy violations and interference with data integrity can be identified for forensics, regulatory, eDiscovery,

7. Ponemon: Quantifying the Value of Unified Endpoint Data Management

and compliance investigations. And, inSync provides organizations the ability to designate a legal/compliance administrator who, under specific guidelines, can override privacy controls to allow select personnel assigned by general counsel to enforce data governance.

Delegated administration capabilities include geo-defined governance features that ensure data privacy. Customers can support varied regional data privacy requirements within a single cloud solution by restricting data access to users or administrators in specific geographies. This geo-specific capability is critical for global organizations, such as those with operations in Germany, whose DPA mandates stringent employee data regulations, including a ban on data storage outside the country.

Leveraging Amazon's AWS cloud infrastructure offers inSync customers the option to have their data in eight different regions around the world including North America, Europe, Asia Pacific, and South America. As an example, a customer with users in Germany would back up data to the AWS cloud in Germany. This customer can create a delegated administrator — an admin physically located in Germany who will manage the German set of employees. A global administrator relinquishes visibility controls so they cannot view the data in Germany. A German administrator could also be designated, who would have no visibility into the data, but would have the ability to control backup and recovery. This allows us to meet strict regional requirements around keeping data private and storing it where it needs to be, thus enabling companies to do business globally.

Conclusion

In today's changing global landscape of data privacy, it's important to know the key issues to consider for complying with data residency laws and protecting corporate and employee data privacy. Companies now need to not only govern and protect data, but also ensure that cloud service providers meet stringent data privacy guidelines for storing data in the cloud. Cloud providers are advancing to keep ahead of these challenges and ensure privacy and security of sensitive enterprise data, so your business can take advantage of the latest benefits of cloud- and mobile-enabled business transactions and avoid serious reputational, financial, and legal consequences.

Data Privacy Readiness Test

Review the following requirements for data privacy for any data stored in the cloud.

How is your organization keeping up?

Regional Privacy

Data Residency: Does your IT admin have the ability to determine regions for data storage?

- ○ Yes
- ○ No
- ○ I don't know

Local Admin: Can IT admins be segregated and delegated with pre-defined granular access rights?

- ○ Yes
- ○ No
- ○ I don't know

Vendor Production: Are vendors prevented from accessing stored data or metadata?

- ○ Yes
- ○ No
- ○ I don't know

Employee Privacy

Individual Privacy: Can end users control privacy settings or opt out of admin data, metadata or audit trail visibility?

- ○ Yes
- ○ No
- ○ I don't know

Data Segregation: Is data on laptops and smart devices containerized?

- ○ Yes
- ○ No
- ○ I don't know

Employee (DPA): Are there exclusionary settings for the data backup and collection process, with admin visibility to audit trails restricted via policy?

- ○ Yes
- ○ No
- ○ I don't know

continued on the next page

Data Privacy Readiness Test

Corporate Privacy

Officer Data: Are there policy group settings for classes via Active Directory (Officers, Legal, etc.) to restrict data visibility?

- Yes
- No
- I don't know

Data Auditing: Can data be fully audited for compliance monitoring for PHI and PII?

- Yes
- No
- I don't know

Tracking & Monitoring: Is monitoring proactive and based on data classifications?

- Yes
- No
- I don't know

Scenario-based Privacy

Compliance: Are there delegated roles for compliance and legal counsel?

- Yes
- No
- I don't know

Investigations & eDiscovery: Is there full data and audit trail access for addressing the unique privacy requirements posed by compliance, investigation and litigation?

- Yes
- No
- I don't know

If you answered "**No**" or "**I don't know**" to more than a few of these questions, it's time to look into strengthening your data privacy stance.

About Druva

Druva is the leader in data protection and governance at the edge, bringing visibility and control to business information in the increasingly mobile and distributed enterprise. Built for public and private clouds, Druva's award-winning inSync and Phoenix solutions prevent data loss and address governance, compliance, and eDiscovery needs on laptops, smart devices and remote servers. As the industry's fastest growing edge data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44(0)20.3750.9440
APJ: +919886120215
sales@druva.com
www.druva.com

Q415-CON-10460