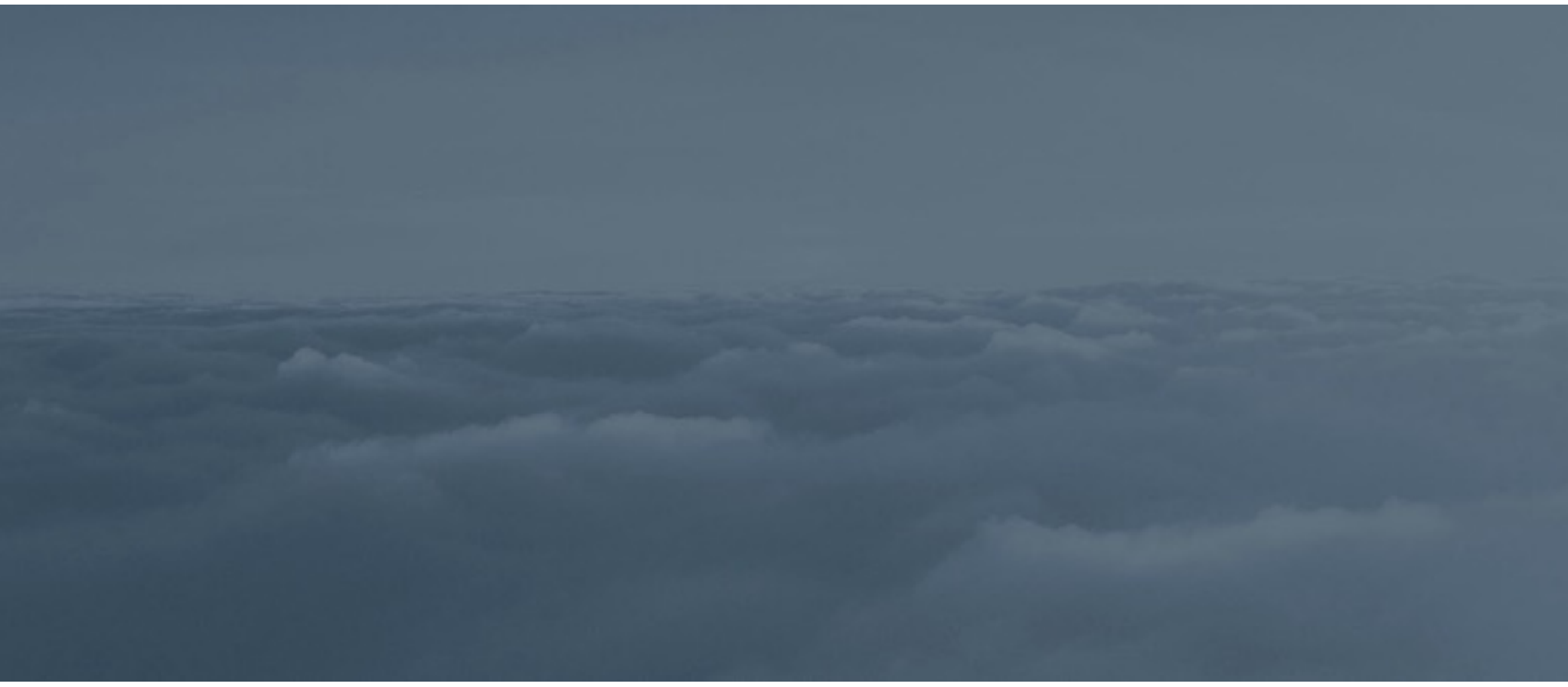
The Data Security Checklist for Business

How to know if your sensitive data is safe in the cloud



ownCloud

Introduction

Increasingly, users are turning to consumer-grade file-sharing services like Dropbox to share and store sensitive corporate data. Users rely on these services to do their jobs, yet companies can't afford the risk that comes with these solutions.

With the cost of data breaches running into the millions, it’s essential to know: Are these cloud services safe for handling your organization’s sensitive data? Data privacy regulations are increasingly important to understand and navigate. Does your cloud service provider (CSP) meet your specific data privacy requirements?

The European Union (EU) has a long history of laws relating to data privacy, both at individual country levels and at an overarching EU level. With the recent ruling by the European Union Court of Justice striking down the EU-US Safe Harbor Act, the importance of data privacy and control over it, as well as the local country regulations that your data is subject to, should be front and center in every IT manager’s mind. Is your CSP up to date on your specific regulatory requirements? Do they meet them?

These are the questions this paper is designed to help you answer. The checklists on the following pages will guide you through the issues involved, assess your own risk and exposure, and help ensure that you maintain the needed levels of security, compliance, and governance.

First, why is it so important?

As an IT manager, you are charged with protecting all sensitive data, proving it is protected, and meeting all compliance requirements along the way. You have to worry about...

- **Data Sovereignty**: Data sovereignty is the concept that information which has been converted and stored in digital form is subject to the laws of the country in which it is located. It's your responsibility, whether you store your files on-premise or in the cloud. Understanding legislative obligations is critical in technology decisions.

- **Security**: Data security is a mandate and consideration must be given to security protocols and processes for each of your use cases, including access control, metadata residency, and key management. Many Content Delivery Networks (CDNs), protocols such as WebDAV, and other web access won't work with encrypted data. Know the security and encryption capabilities available to protect your data.

- **Control**: Your enterprise security protocols and processes may disappear when you hand over your data to an outside vendor. In addition to controlling access, the ability to manage, monitor and log activity should be comprehensive, and backup and rollback capabilities are a must-have.

A failure in any of these areas can cause immeasurable damage including losses of IP, brand value and more. In fact, even if no actual breach occurs, a failed regulatory audit can do serious damage, and cost millions in fines.

To protect your data and your business, you need to ask some hard questions ...

Is the hardware under your control?

Hardware Checklist

- ✓ Where does your hardware reside, and who has access?
- ✓ How is physical access granted and revoked?
- ✓ Who has administrative access, and how is it managed?
- ✓ How is access controlled, audited and logged?
- ✓ How do your governance policies line up?
- ✓ What data sovereignty laws are you subject to?
- ✓ How is the hardware backed up, patched and updated?

Security starts with the hardware. If you give up control to a third-party, you need to confirm that security standards are being met – to your standards as well as that of governing legislation. Further, you must be certain your service level agreements with your users will be maintained.

Ultimately, you need to be able to prove at any time who has had access to your servers and why.

Be sure to read the fine print, ask for proof, and visit the the facilities if you can. Do whatever you would do to certify a new facility on your own premises. In each member country of the EU, you are ultimately responsible for data security, even if it is hosted and stored on third-party hardware, in a third-party data center.

Where does your data go?

Network Checklist

- ✓ Where are the endpoints, and who has access?
- ✓ Where do your files go when in transit and how are they protected?
- ✓ What happens in a DR / failover situation?
- ✓ Is the network in compliance with your policies?
- ✓ How do you know when an intrusion is detected?
- ✓ What is listening to / analyzing your traffic?
- ✓ Are CDNs in use to accelerate traffic? Which ones?
- ✓ Can traffic be encrypted with your CDN?

Network questions are similar to the hardware issues, but even more complex.

One little understood issue is the CDN, or Content Delivery Network. It is entirely possible that a CDN will be part of a chain leading to an unencrypted file at a third party data center. And then you have to ask the same set of questions all over again. You need to find out through the entire chain of CDNs if there could be unencrypted access at any point.

Network monitoring should provide you the answers required to meet compliance requirements. Remember — you can be at risk even if no breach has occurred. Not knowing can be enough to get you in trouble.

Where does your data live?

Storage Checklist

- ✓ Where are files stored, and who has access?
- ✓ Are files being scanned when they arrive?
- ✓ What sort of retention and tracking are in use?
- ✓ What if you want your files back?
- ✓ What if the government asks for your data?
- ✓ How is encryption handled? Who has the keys?
- ✓ What happens when you delete your files? De-dupe?

Storage issues are especially sticky. Start with who owns the data. Some user license agreements make the service provider the owner of data. That means they're obligated to turn over the data if the government asks for it. Some data sovereignty legislation puts the risk on you, even if your data is hosted with a third-party. Know your rights…and your risks.

Then there are technical issues. Some cloud vendors access files for scanning and de-duping, which is actually illegal in certain countries and jurisdictions for certain types of files. Make sure key management is tightly controlled. And be careful about deletions—it is possible that some files are not truly deleted or that components of files are left behind during de-duping, which could still leave you in breach.

Who uses your data?

Users & Admin Checklist

- ✓ How are users provisioned, authenticated? SSO?
- ✓ How are admins trained, screened and monitored?
- ✓ Do admins follow your policies, or theirs?
- ✓ How are users tracked and audited?
- ✓ What sort of user logs are available to set alerts?
- ✓ Can users or admins circumvent your IT policies?
- ✓ How are user keys maintained? Restored? Who has access to them?

Of necessity, service providers train their personnel on a one-size-fits-all basis. The people are probably well trained on the service providers' procedures, but not on **YOUR** policies and procedures. If you have a unique need in any of these areas — hardware, network, storage, backup, users and admin—the provider probably cannot make it happen.

You need access to user logs and the ability to incorporate them into your own tools. If you depend on the service provider to supply that, remember that their failure could be your failure in an audit. You also want to be sure that you are in control of your keys as this may determine who is ultimately in control of your data.

Does it all work together?

Integration Checklist

- ✓ Are your governance policies followed?
- ✓ Must you expose files to the cloud to access them?
- ✓ How do you leverage existing IT investments?
- ✓ How can you leverage existing IT tools and procedures?
- ✓ What databases can be used for your data?
- ✓ What storage can you work with for your files?
- ✓ Is this another silo of data you have to manage?
- ✓ How can you support future requirements?

Your IT organization may have spent years building out an organization and structure that meets regulatory requirements, retention policies, deletion processes, and your own high standards.

If you can’t integrate and leverage those solutions for your file sharing, then a lot of your investment has been wasted. And, you’re getting a new silo of data.

It’s possible to integrate outside services by opening a new hole in your firewall, but that is not ideal. Further there will always be data that you can’t let out, so there will always be a separation between the cloud service and what you’re trying to do internally.

Understanding how you can support future requirements will help you make the best decision for your organization today.

Do you comply with the law?

Regulatory Checklist

- ✓ Do you know who is responsible for securing your sensitive data?
- ✓ Are you a multinational organization, playing by different rules?
- ✓ Does your provider comply with your regulations?
- ✓ Is your provider a wholly-owned subsidiary of a US corporation?
- ✓ Is your provider EU Data Protection Directive/BDSG/PRISM/FISA/etc. proof?
- ✓ Do you own the files stored with your provider?
- ✓ Are you able to comply with data protection laws?
- ✓ Can you prove you are in control of your data?

The last is the core question every enterprise needs to ask: Can you prove you are in control? If so, you are in good shape. If not, it is probably time to re-evaluate.

Regulations are all about knowledge and control. Loss of control at any given time on a given file could be a problem in an audit, and real trouble in the event of a breach.

Regulatory compliance comes in many forms, and you need to be aware of how laws outside of your own country may impact your company's data privacy. An example of this has to do with subsidiaries of US corporations. Regardless of where a company's office is outside of the US, if the company owning the subsidiary is a US company, the US PATRIOT Act can be invoked and personal data may be at risk.

There are both EU umbrella agreements and country-specific regulations to consider. EU-wide regulations include the Data Protection Directive which regulates the gathering and transfer of personal data outside of the EU, and the EU-US Safe Harbor Agreement. The Safe Harbor Agreement was struck down by the European Court of Justice in October 2015. With this agreement gone, the data protection authorities in the 28 EU Member States may not allow data transfer to US companies that are subject to mass surveillance laws such as PRISM and FISA.

Additionally, each of the 28 EU Member states have country-specific laws that must be complied with.

Understanding how your service provider complies with your data protection laws is critical to the safety and control of your data.

Service providers can and do take serious measures to secure your data. But in the end, it is your data, and there will always be a risk in putting your data outside your company.

An Alternative Approach

For enterprises that want and need definitive, full control of their data, there is an alternative approach that still delivers the benefits of the cloud.

In this approach, the control plane for file sync and sharing resides on-premise within your corporate data center or that of your trusted local service provider. Regardless of where the data is stored, the encryption keys, metadata and access control is onsite. That means that even if you are mandated to share data, you cannot be forced to turn over the encryption keys required to decrypt it. ownCloud is the only EFSS vendor to provide IT with a storage choice and make this possible for the enterprise.

This solution runs on a scalable platform with full enterprise file sharing, and with the extensible integration to all of IT's established systems, policies and standards.

Meanwhile, to users of the system who simply want to share information with their colleagues and communicate more productively, the system looks and acts like consumer-grade cloud services. This leads to user adoption of a secure file sharing solution that offers the security and compliance needs mandated by EU-wide and your country-specific laws.

To find out more about this approach, visit www.owncloud.com.

Appendix

Helpful Links on EU Data Privacy Laws:

EU Data Protection Directive:
http://ec.europa.eu/justice/data-protection/

Data protection bodies:
http://ec.europa.eu/justice/data-protection/bodies/index_en.htm

Data protection legislation:
http://ec.europa.eu/justice/data-protection/law/index_en.htm

Handbook on data protection laws:
http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

Data residency, data sovereignty blog:
https://owncloud.com/data-residency-data-sovereignty-and-the-mad-scramble/