Acronis

The Dissolution of Safe Harbour and What It Means for Your Business

Table of Contents

Introduction

In an October 28, 2015 research article published by the **451 Group, Penny Jones,** Senior Analyst, European Services writes[1], "There have been numerous reactions to the EU Court ruling. While the overall message from data protection authorities (DPAs) in EU countries and the US has been to remain calm, there has been a lot of concern from those that relied upon Safe Harbour to do business…"[2]

If your organisation is a European company that stores some or all of its information in the cloud, and this information may be accessed or stored outside of the EU, you may be scrambling for a way to respond to the recent European Court of Justice (ECJ) ruling that dissolves the Safe Harbour agreement. If this is the case, we have prepared this white paper to give you guidance on:

- Why the ruling was made and why is it important
- What it means for European-based companies and European-based cloud providers
- Why European Acronis' data protection products adhere to the new ruling
- The five steps to follow to audit your company's business and mitigate the risk of your data being stored on US soil

[1] *Jones, P. (2014). EU says 'don't panic'? but what will keep you safe now that Safe Harbour can't?.* Retrieved from 451 Research Group.

[2] *Acronis does not in any way endorse the conclusion made in the article as conclusions or positions of Acronis.*

Why the Dissolution of Safe Harbour?

Whether consumers are aware of it or not, trans-Atlantic data flow has become essential to how consumers interact with businesses and how businesses operate. In this age of technology, the internet connects all of us virtually and by extension, the cloud has torn down borders across the globe, making it possible to share information with anyone, in real-time, wherever they are.

With the exposure and risk of data loss and theft, countries have implemented various regulations and laws to protect personal information. Up until recently, most consumers trusted major brands and companies with their data without knowing how it was stored or who had access to it. However, ex-NSA consultant, Edward Snowden, and others put a spotlight on this issue. The primary driver for this increased awareness is the revelation and concerns about the extent of US government spying and monitoring of personal information.

Whilst the debate has carried on these past few years, major companies and famous brands had a variety of reasons to store their data in the US. Perhaps it was cheaper or it was just easier to keep the "status quo" because the Safe Harbour Agreement guaranteed a level of protection for EU data transferred to United States Data Centres.

> However, the ECJ's ruling that the Safe Harbour agreement, which allowed the transfer of European citizens' data to the US, is invalid has thrown the data protection landscape into flux.

It is the opinion of EU lawmakers that US data protection laws don't match EU standards. Their recent ruling, which invalidated the Safe Harbour Agreement, centred on their concerns with the US Patriot Act. The Patriot Act permits the US government to access and monitor any data stored in the US, making it possible for defence agencies to share information and monitor for potential terror threats.

European and US companies both viewed the Safe Harbour agreement as a "safety net" permitting the transfer of EU data to the US. It permitted any company to self-certify that they would protect EU data when transferred and stored within US data centres.

The Impact on European-based Companies

It may not be clear and apparent to many customers what type of data is collected, let alone where it may be stored. More importantly, the definition of what constitutes personal information varies between countries. Companies can leverage consumer information for lucrative ad targeting in the US, or leverage corporate data archived in the cloud for future reference and compliance purposes. According to **IDC**, these cloud data models are on the rise. European businesses are expecting to spend **$8.2 billion** on professional cloud services in 2015, an increase from only $560 million in 2010. Outsourcing to the cloud has been economically sensible for some time so it's no surprise that as many as **4,000 firms** will be affected by the ECJ ruling.

> For companies doing business in the US, simply setting up a data centre in the EU will not solve this problem. The US Government may still reach and access this data.

As a result, IT managers and businesses in Europe find themselves thinking – how does this affect me?

Since news outlets have portrayed this landscape as chaotic, businesses are challenged to just "keep calm and carry on." Businesses that outsource data storage to US-based companies need to evaluate the risks of compliance with heightened European protection laws. Failing to comply with the more stringent data privacy regulations can jeopardise their relationships with customers and ultimately their reputation.

This is just the tip of the iceberg. Complicating the landscape further is the rising use of shadow IT, which has been recognised **by Gartner** as a **growing and unstoppable force**. Shadow IT, such as Dropbox, let employees use convenient, file sharing solutions, which utilise US-based storage systems. Shadow IT is often not sanctioned by the IT department and originated as a way for employees to get around existing systems. Indeed, **CipherCloud** found that as many as **86 per cent** of cloud applications used by enterprises can be classified as unsanctioned shadow IT.

As a result, it's not always obvious if US-based storage models are being used and IT departments across Europe have a fair amount of detective work on their hands if they are to rectify this situation.

Instead of changing where data is stored, most companies will propose contract amendments

reassuring customers that they meet heightened data privacy laws that permit the continued transfer of EU personal data outside of the EU. However, most consumers and small-to-medium businesses (SMBs) do not have the funds to hire attorneys to review these contracts to ensure it truly protects the customer and is in compliance with these stricter regulations. These consumers and SMBs are, once again, trusting these companies will protect the data, but there is still risk since the data is transferred and accessed outside of the EU.

Customers might, quite rightly, ask where their data is stored, regardless if the company meets the heightened regulations. While the invalidation of the Safe Harbour is confusing enough, explaining the alternatives may be an impossible battle. This can lead to customers seeking EU-based storage models as a more conservative approach rather than trusting that their vendors' security measures are in compliance.

A Silver Lining for European Cloud Providers

US-based companies will have more trouble complying with stricter regulations. As a result, some European businesses are considering a switch from storing data in the US to storing their data in the EU. This provides a huge opportunity for EU-based service providers.

Every cloud has a silver lining and that's certainly the case here. Businesses are becoming more aware of the benefits of storing data in the EU. European technology firms are developing innovative cloud-based solutions, specifically designed to meet the needs of European businesses.

Acronis, a Swiss-based company, has been developing innovative technology for over 12 years. Its cloud-based solutions provide its customers with the option to store their data in a variety of data centres in the United Kingdom, France, and Germany with additional EU locations opening in the near future.

Acronis has proven solutions to fulfil the need for a powerful, affordable and safe data backup option — a challenge experienced by many European businesses today.
Storing data in Europe has the added benefit of keeping customer information simple; it is kept in the EU and avoids the complication of international data transfer. For European businesses, this means intellectual property is guaranteed a certain level of security and for customers, personal data is guarded and respected as just that — personal.

What the Safe Harbour Dissolution Means for Acronis Customers

It is fair to say there is a deluge of data concerns coming to the surface. For businesses looking to keep operations running, the Acronis philosophy of storing its EU customers' backed up data in EU data centres is a welcome breath of fresh air. Acronis' EU customers have the opportunity to choose from a variety of EU data centres. If an organisation previously chose to store its backups in a non-EU datacentre, Acronis has plenty of capacity and can assist the organisation to migrate the data to one of its EU data centres.

Acronis Access Advanced

The Acronis Access Advanced solution for business is an intuitive solution that is designed to protect data and, by extension, a business' reputation and competitive position.
Acronis Access Advanced is an easy, complete, and safe access, sync, and share solution, providing IT with complete control over business content to ensure security, maintain compliance, and enable BYOD (Bring Your Own Device). Employees use any device to securely access corporate files and securely share content with other employees, customers, partners, and vendors.
Acronis Access Advanced is an on-premises solution that gives an IT department 100 per cent control of its data and everything IT needs to protect, control, and manage mobile files and content.

> Unlike US-based options such as Dropbox, data is not transferred to the US with Acronis Access Advanced

Data Security and Privacy

Acronis Access Advanced also provides additional features to ensure the security and privacy of its customers' data including:

- Highly granular policies to control files, users, and devices; over fifty security and user permission policies are available to satisfy the most demanding customers.
- Integration with Microsoft® Office, which allows users to securely create and edit Microsoft Office documents and annotate PDFs within Acronis Access Advanced.
- Secure over-the-air and on-device FIPS 140-2 certified encryption ensuring that only authorised individuals can view and access data.
- Selective remote wipe removes documents from shared mobile devices.
- An audit trail and history of all transactions, which includes search, filter, and export functions, shows who accesses content, when, what they did, and with whom content was shared for quick troubleshooting and compliance / audit support.
- White and black lists of users, groups, domains, and applications provide flexibility when determining and managing who can access the data.

Data privacy and security is not the only differentiating feature of Acronis Access Advanced; it is also the easy-to-use and the most complete file sync and share solution on the market.

Ease of Use

Acronis Access Advanced is an easy solution for enterprises to administer and use:

- Allows employees to easily and safely create new documents and edit content that resides on file servers, NAS, and SharePoint® using popular mobile devices, Macs, and PCs.
- Offers a simple-to-use, intuitive user interface; employees require virtually no training to use it.
- Easy-to-use, yet highly granular security and privacy features ensure that data is always safe.

Complete

With Acronis Access Advanced, companies can turn mobile devices into a natural extension of their business:

- Integrates with Active Directory® for authentication, user management, and device enrolment.
- Provides full support for BYOD, enabling mobile users to access their work from their own devices:

  - iPad® 2, 3, 4, mini and Air, iPhone® 3GS, 4, 4S, 5, 5C, 5S, 6/6+ iOS 6 or later, Android® Phones & Tablets, Windows®, Mac®

  - Web Browsers: Firefox®, Internet Explorer, Google® Chrome™, Safari®
- Integrates with key mobile device management (MDM) partners including MobileIron, Good Technology, and others to deliver a complete enterprise mobility strategy.
- Synchronises content from file servers and SharePoint to Macs and PCs, providing users with greater flexibility to work on their choice of devices.
- Provides web access to content on file servers and SharePoint, making it easy for users to find what they need.
- Includes a web API that IT can use to build custom apps and integrate Access into other products using standard Web Service calls.
- Drives productivity across the enterprise with capabilities that are easy to learn and use.

Acronis Access Advanced offers the most advanced, secure file sync and share solution to improve employee productivity, enhance customer service, and enable BYOD — all without migrating data to US soil (if the customer chooses not to).

Acronis Backup Service

When it comes to backing up data, Acronis, with its European-based data centres, can protect information as well as business reputations.

The Acronis Backup Service helps to protect business data by backing it up with a complete solution designed for today's diverse IT environments. Centralised management from the EU-based cloud makes set up easy and reduces IT workload. The service eliminates the complexities associated with competitive cloud solutions, as well as the data protection woes that are now part and parcel of using US-based backup solutions. It allows for business continuity in every sense.

With local and cloud backup available, businesses using the Acronis Backup Service can enjoy all the benefits of hybrid protection, plus the ability to recover an entire system on demand. Complete and easy to use, Acronis Backup Service backs up data from any source and recovers data to any destination and system.

Data Security and Privacy

All Acronis Data Centres are Tier-IV designed. Acronis physically secures its data centres with high fences, 24x7 security personnel, and video surveillance with 90-day archiving. Biometric hand-geometry scan and proximity key cards are required for access.

Acronis Backup Service supports AES-256 encryption, which is a government-approved standard for security encryption. Users can set up their own unique password and encrypt data when it is at rest and when in transit to the Acronis Cloud via a secure channel using 2048bit SSL management channel.

No one can intercept or access the data while in transmission or once it is stored in the cloud — not Acronis or any other organisation or agency.

Acronis Backup Service addresses the challenges associated with the dissolution of Safe Harbour. Your data never leaves the EU, nor can it be accessed outside of the EU.

An Easy-to-use, Complete Service

Acronis Backup Service provides an easy-to-use, browser-based console that allows centralised and remote management of backups and recovery. The services offers patented disk and VM image backup so you can rapidly back up and maintain a complete image of a disk or volume on a physical or virtual machine in one easy step. This lets you quickly capture any data, store it on any storage device and in the cloud, and recover it to any platform, hypervisor, or operating system.

Acronis Backup Service supports virtual and physical Windows®/Linux/Mac environments, VMware®, Microsoft®, Citrix®, Red Hat®, Linux KVM, and Oracle® hypervisors; and Microsoft Exchange, SQL Server, and System State. With this service, you can also:

- Recover a complete system to bare metal or just recover selected files and folders.
- Recover to the same or dissimilar hardware or hypervisor.
- Secure data off-site with an initial seeding programme that quickly moves large volumes of data to the cloud.
- Enjoy agentless backup for VMware and Hyper-V, eliminating the need to install an agent on each VM, simplifying deployment and reducing management complexity.
- Easily update agents on workstations, physical servers, and virtual machines from within the management console.
- Reduce management efforts and the load on production services with backup staging support for disk-to-disk-to-cloud schemes.

With Acronis Backup Service, an organisation can protect its business and start backing up its data in no time with a quick and easy-to-use service that eliminates the complexity, costs, hardware, and resources required to manage an on-premises solution. Most importantly, this service ensures that the data is stored in an EU-based data centre.

Conclusion

With media attention currently concentrated on the Safe Harbour issue, data privacy and protection is something close to the hearts of companies across Europe. It's vital that businesses protect themselves and their customers. Acronis solutions are an important component of a total strategy that helps an organisation address the data privacy issue.

If your EU-based organisation is a current Acronis Access Advanced and Acronis Backup Service customer, you are already ahead of the curve. Still, we encourage you to evaluate your data protection policies and how you store your data.

If your EU-based organisation is not an Acronis user, here are five steps you can follow to mitigate risk and put safe and compliant procedures in place to protect your data. With your reputation on the line, data protection is not something that you can afford to get wrong.

Five Steps to Help Mitigate Risk

If you are reading this article, you may be wondering what to do. So, here's some advice — review your internal systems and check that you are on the right side of the law.

1. **Know what happens to your data —** ask yourself this question and make sure you and your colleagues have visibility into exactly what data is moving outside your network, where and when.
2. **Be aware of where in the world your backup data is —** some businesses back up locally, some use cloud as part of a hybrid solution, and others opt to just use cloud. If you are using a cloud solution, be sure to ask your cloud provider where their data centres are based and leverage their local EU data centres where possible. You should evaluate data protection on a case-by-case basis. And ensure it is controlled and processed in the EU.
3. **Prepare to be quizzed by customers —** with the dissolution of Safe Harbour hitting the headlines, be prepared to address customer questions about where their personal data is stored. Talk to sales staff and customer support and make sure they have all of the information they need.
4. **Audit employee data-sharing habits —** check with your IT department to be sure it has full visibility of the shadow IT and cloud usage that's taking place outside of IT's control. Where this is happening, determine where all the data centres are located and which employee habits need to change in order to comply with ECJ Safe Harbour ruling.
5. **Question your cloud services provider —** future-proof your IT by selecting to work with vendors that can provide you with a flexible, secure, EU-based cloud infrastructure. If your current providers cannot meet your requirements, it might be time to look elsewhere.

Acronis

References for Safe Harbour White Paper

Abutaleb, Y., Fioretti, J. (2015). Smaller U.S. businesses fear freeze from EU privacy ruling. Retrieved from http://www.reuters.com/article/2015/10/08/us-eu-dataprotection-idUSKCN0S12TL20151008#edIAVxZtJd58gCOv.97

Amirtha, T. (2015). Safe Harbor was for EU privacy: But how safe is US data in Europe? Retrieved from http://www.zdnet.com/article/safe-harbor-was-for-eu-privacy-but-how-safe-is-us-data-in-europe/?tag=nl.e539&s_cid=e539&ttag=e539&ftag=TRE17cfd61

CipherCloud Report. (2015). Cloud Adoption & Risk Report in North America & Europe – 2014 Trends. Retrieved from http://www.ciphercloud.com/company/ciphercloud-report-identifies-1100-cloud-applications-use-companies-86-percent-cloud-applications-shadow/

Cloud Security International. (2015). Shadow IT continues to give cause for concern. Retrieved from http://cloudsecurityinternational.info/news_full.php?id=36893

InfoCuria - Case-law of the Court of Justice. (2015). Judgment of the Court (Grand Chamber). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031

Jones, P. (2015). EU says 'don't panic' – but what will keep you safe now that Safe Harbour can't? Retrieved from: 451 Research Group

Kepes, B. (2015). How tech vendors are reacting to the Safe Harbor ruling. Retrieved from http://www.networkworld.com/article/2991752/cloud-security/how-tech-vendors-are-reacting-to-the-safe-harbor-ruling.html

Mingay, S. (2014). Embracing and Creating Value From Shadow IT. Retrieved from http://www.gartner.com/technology/reprints.do?id=1-2AG5N3Q&ct=150223&st=sb

Mizroch, A. (2015). U.S. Tech Firms Look To Data Centers on European Soil. Retrieved from http://blogs.wsj.com/digits/2015/10/06/u-s-tech-firms-look-to-data-centers-on-european-soil/

Pardau, S. (2015). European Court of Justice Strikes Down U.S.-EU Safe Harbor. Retrieved from http://www.marketingresearch.org/article/european-court-justice-strikes-down-us-eu-safe-harbor

Scott, M. (2015). As U.S. Tech Companies Scramble, Group Sees Opportunity in Safe Harbor Decision. Retrieved from http://www.nytimes.com/2015/10/21/technology/as-us-tech-companies-scramble-group-sees-opportunity-in-safe-harbor-decision.html?ref=business&_r=2

About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile. Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com**.
Follow Acronis on Twitter: **http://twitter.com/acronis**.