Accellion

After EU Safe Harbor: New Strategies for Compliance

Executive Summary

Personally Identifiable Information (PII) is information such as a name, address, and/or telephone number that can be used to identify a specific person. PII is essential for commerce, healthcare, and government; it is used for everything from payroll to patient records to benefit disbursals.

In the European Union (EU), where laws recognize a citizen's general right to privacy, PII is protected. The EU's Data Protection Directive (Directive 95/46/EC) sets forth strict rules for the collection and use of PII, based on the principles of transparency, legitimate use, and proportionality. All EU companies collecting and using PII must comply with the Data Protection Directive's rules. For example, companies must use PII only for the purpose stated when the data is collected, and they must allow individuals to review and correct any PII being stored.

When EU PII is transferred to a U.S. company, that company must agree to comply with EU data privacy laws. From 2000 to October 2015, the most common way to demonstrate compliance was through the EU-U.S. Safe Harbor Agreement, which allowed U.S. companies to self-certify that they complied with EU data privacy laws. Since the Safe Harbor Agreement was passed, about 4,500 U.S. companies managed their EU data privacy compliance this way. Many international companies, including Facebook and Google, used Safe Harbor to claim compliance with data privacy regulations while collecting and using the PII of EU citizens.

On October 6, 2015, the European Court of Justice (ECJ), the highest court in Europe, struck down the Safe Harbor Agreement, saying that it did not protect the private data of EU citizens. The ruling stated that the agreement failed to comply with EU privacy laws because it allowed EU PII stored by U.S. companies to be accessed and analyzed by U.S. intelligence agencies as part of their mass surveillance activities. In nullifying Safe Harbor, the Court specifically cited the revelations of former National Security Agency (NSA) contractor Edward Snowden about the extent of U.S. surveillance. As a result, the Court decided that companies could no longer use Safe Harbor to demonstrate compliance with EU data privacy rules. Following the Court's judgment, EU regulators set a deadline of January 31, 2016 for the U.S. and the EU to implement a new agreement that would genuinely protect the privacy of EU citizens.

On February 2, 2016, the European Commission and the U.S. Department of

Commerce announced a new agreement called Privacy Shield. The new agreement seeks to end the mass surveillance of EU citizens and to give those citizens the ability to formally complain about any privacy abuses by U.S. companies. The U.S. Federal Trade Commission (FTC) has committed to enforcing compliance with the new agreement. Further, U.S. and EU officials will review data collection activities once a year.

The Article 29 Working Party—the chief data privacy organization in the EU—has yet to review and approve the new agreement. Assuming they receive the details of Privacy Shield soon, they hope to complete their legal analysis by April. In the meantime, they intend to continue investigating privacy violations and enforcing penalties for non-compliance.

Until Privacy Shield or some other future agreement is officially approved, how should U.S. companies and other organizations act to support compliance with EU data privacy regulations?

Here are three strategies that companies should consider implementing, regardless of the status of Safe Harbor or Privacy Shield:

- Strategy #1: Audit internal PII practices.
- Strategy #2: Review content storage and distribution policies to ensure that EU data is kept within the EU.
- Strategy #3: Deploy private clouds to keep EU data local.

A private cloud is a cloud service that is hosted either on-premises in an organization's data center or in a local third-party data center where the organization has full control over data security and data governance. Ideally, this should include sole possession of data encryption keys.

kiteworks is a Secure Content Platform from Accellion that enables enterprises to provide users with powerful content management and collaboration features, while complying with strict data privacy regulations such as the Data Protection Directive. The kiteworks platform offers enterprise organizations a secure file sharing and collaboration solution that enables secure internal and external sharing of enterprise information, and a development platform for designing and deploying custom enterprise applications to increase productivity, while ensuring data security and compliance.

Accellion is the leading provider of private cloud solutions, providing organizations the opportunity to leverage cloud computing infrastructure and resources while ensuring that data is not co-mingled. An industry first, Accellion's kiteworks platform offers a multi-tier architecture that enables IT organizations to distribute cloud services across countries to optimize regulatory compliance and business performance.

For more information about Accellion and kiteworks, please visit www.accellion.com

The Rise and Fall of the Safe Harbor Agreement

Data Privacy and the EU Data Protection Directive

Nearly 510 million people reside in the European Union (EU), and all of them have private data including, but not limited to: mailing addresses, IP addresses, phone numbers, bank account numbers, and health records.[1] Because this information can be used to identify a specific person, privacy regulations refer to this type of data as Personally Identifiable Information (PII).

For the past twenty years, the EU has recognized that its citizens have the right to control their PII. The legal framework for protecting PII is the Data Protection Directive (Directive 95/46/EC), which the European Commission passed on October 24, 1995. Under the directive, data processing is only lawful if a private citizen has given his or her consent or if for some reason the processing is necessary for legitimate reasons. Private citizens have the right to ensure their data is correct, and in many cases, they even have the right to withdraw their data from use.

The Data Protection Directive's rules for the use of PII are based on three broad principles:

- **Transparency**
  Citizens have the right to know when and how their data is being "processed" (that is, collected and used), and they have the right to know exactly who is processing it.

- **Legitimate use**
  PII must only be used for legitimate purposes. Data controllers (organizations collecting and processing PII) should handle as little personal data as possible. If data is being collected for statistical or historical analysis, efforts must be made to ensure the data is accurate and the data should include as few personal details as possible. Controllers for example are prohibited from processing data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life," except under strict conditions.

- **Proportionality**
  The amount of data collected must be reasonable given the purpose of its collection. Controllers should not collect and store more data than is strictly necessary for their purpose. Also, controllers cannot process data for selfish or spurious reasons.

The Data Protection Directive applies to all 28 Member States of the EU. Interpretation and enforcement of the directive is the responsibility of a Data Protection Authority (DPA) in each country. For instance, when German citizens are concerned about how their data is being handled, they can file a complaint with the DPA in Germany. Or, if their complaint concerns a company based in Spain, they have the option of filing a complaint with the DPA in Spain.[2]

1 http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00001&plugin=1
2 The European Court of Justice is hearing a case that raises the question of just which DPA has jurisdiction in cases like this. http://www.theregister.co.uk/2015/10/01/eu_data_protection_court_case/

The U.S.-EU Safe Harbor Agreement

The Data Protection Directive clearly protects the private data of EU citizens when that data remains in Europe. What about data that is transferred to international companies or companies in other countries?

Under the terms of the directive, the PII of EU citizens may not be transferred outside the EU unless the country receiving the data—a "third country" in the language of the directive—has agreed to uphold the principles of the directive. In other words, "third countries" need to abide by the same rules as EU member states. And "third countries" include the U.S., which is the largest trading partner of the EU.[3]

To make it easier for U.S. companies such as Facebook, Google, and Apple to handle PII from EU citizens without undertaking repetitive, time-consuming negotiations and inspections, the U.S. and the EU negotiated a Safe Harbor Agreement in 2000. Under this agreement, if U.S. companies certified themselves as compliant with the principles of the Data Protection Directive, they could legally become controllers of PII belonging to EU citizens. As the European Commission noted in June 2015:

> *While signing up to Safe Harbour Privacy Principles and FAQs is voluntary, these rules are binding under U.S. law for those entities that have signed up to them and enforceable by the U.S. Federal Trade Commission…. The Member States' Data Protection Authorities (DPAs) remain empowered and obliged to examine, with complete independence, whether data transfers to a third country comply with the requirements laid down by Directive 95/46/EC.*[4]

In the 15 years since the Safe Harbor Agreement was established, almost 5,000 companies have self-certified to protect EU citizens' PII and uphold the Safe Harbor Agreement.

Aside from the Safe Harbor Agreement, there are two other legal frameworks under which third countries or global organizations can process EU PII outside the EU itself:

- **Standard Contractual Clauses (SCCs),** also known as model clauses or model contracts, set forth the respective obligations of data exporters and importers, including security measures and "notification to the data exporter of access requests by the third countries' law enforcement authorities." The model clauses preserve the right of EU citizens "to invoke before a DPA and/or a court of the Member State in which the data exporter is established the rights they derive from the contractual clauses as a third party beneficiary." In other words, whether their data is exported to a third country under Safe Harbor or under model clauses, EU citizens always have the right to data protections described in the directive.[5]

- **Binding Corporate Rules (BCRs)** invoke data privacy protections for data transfers within the corporate group of a multinational company. "The use of BCRs thus allows personal data to move freely among the various entities of a corporate group worldwide—dispensing with the need to have contractual arrangements between each and every corporate entity—while ensuring that the same high level of protection of personal data is complied with throughout the group by means of a single set of binding

3 http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf
4 https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-566-EN-F1-1.PDF
5 Ibid.

and enforceable rules." Just as they can under SCCs, individuals can file complaints with DPAs if they feel their data privacy rights are being violated under BCRs.[6]

Once again, while some U.S. companies such as Microsoft have opted to manage data transfers under model clauses, most U.S. companies have managed transfers and processing of EU citizens' data through the Safe Harbor Agreement. From July 2000, when the agreement was finalized, until October 2015, the Agreement was recognized on both sides of the Atlantic as a legally binding and practical solution to protecting the data privacy rights of EU citizens while enabling the flow of personal data essential for commerce and government actions in a global economy.

In the age of Facebook, Google, and widespread cloud computing and digital trade, the Safe Harbor agreement made it easy for U.S. businesses to quickly put measures in place for handling large volumes of PII from Europe. By late 2015, the digital trade between the EU and the U.S. was worth $260 billion, and over 4,000 U.S. companies were handling PII daily under the aegis of the Safe Harbor Agreement.[7] [8]

The Safe Harbor Agreement Undone

The undoing of the Safe Harbor Agreement began innocuously enough. An Austrian law student named Maximilian Schrems decided to study abroad and enrolled in Santa Clara University, a Jesuit university located in the heart of Silicon Valley, among some of the world's largest technology companies. One day, a professor of Schrems' invited Ed Palmieri, a data privacy lawyer from Facebook, to deliver a guest lecture. Schrems was astonished by Palmieri's limited understanding of EU data privacy laws. In Schrems' view, Facebook seemed to be taking a cavalier attitude toward the privacy rights of EU citizens.

Schrems began investigating Facebook's privacy practices. He discovered that the company maintains hundreds of pages of data about every user, including users who believe that all their data has been deleted.

Soon Schrems was filing legal complaints against Facebook, claiming that the company was violating the privacy rights of EU citizens. The complaints become troublesome enough that on February 6, 2012, Facebook's European director of policy Richard Allan and another Facebook executive spent six hours meeting with Schrems in Vienna to discuss his concerns.[9]

While Schrems was arguing that Facebook was not taking EU privacy regulations seriously enough, the European Commission was hard at work making those regulations stricter and more consistent. In January 2012, just two weeks before Schrems' meeting with Allan, the European Commission proposed a new directive—a General Data Protection Regulation (GDPR)—to update the Data Privacy Directive so that it now accounted for social networks and cloud services. The new regulation broadened the scope of data privacy regulations to cover any organization anywhere in the world that stored the private data of EU citizens. Now, a single set of rules would apply to all EU members, smoothing out some of the differences in legal interpretation that had arisen among some of the EU's DPAs. Fines for non-compliance would reach up to €1 million or up to 5% of an offender's global revenue, whichever was higher.[10]

6 Ibid.
7 http://www.msn.com/en-us/money/watch/sec-pritzker-europes-safe-harbor-about-protecting-privacy/vi-BBowbKj
8 http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361
9 http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/
10 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

The next major development in the story came courtesy of Edward Snowden, the former National Security Agency (NSA) contractor who in 2013 disclosed the alarming extent to which the NSA and other U.S. intelligence agencies were collecting data of private citizens, including EU citizens. Snowden disclosed that as part of a secret program called PRISM, the NSA was collecting foreign communications traffic from the servers of AOL, Apple, Facebook, Google, Microsoft, PayTalk, Skype, Yahoo, and YouTube.[11] That traffic included the PII of EU citizens.

Schrems recognized that this widespread collection of PII violated the spirit and letter of the EU's Data Protection Directive. Specifically, if intelligence agencies were collecting PII secretly, they violated the Directive's principle of transparency. And if the agencies were sweeping up PII indiscriminately, they violated the principle of proportionality. And, needless to say, EU citizens had no way of knowing their PII was being accessed, no means of asking the intelligence agencies what they were doing with their PII and no recourse to get their PII corrected or deleted. In short, EU citizens had lost all control of their data.

From Schrems' perspective, if the Safe Harbor Agreement allowed U.S. companies to handle the PII of EU citizens and those U.S. companies were going to collude, more or less willingly, with the intelligence agencies collecting this PII, then the Safe Harbor Agreement itself was in violation of the Data Protection Directive.

This is the argument that Schrems took to court, and on October 6, 2015 he prevailed in the highest court of the European Union, the European Court of Justice.

Schrems had litigated against the Data Protection Commissioner of Ireland, where Facebook and Google have their European headquarters. Ruling for Schrems, the Court struck down the Safe Harbor Agreement as "unlawful," because U.S. companies are "bound to disregard, without limitation" the privacy safeguards provided in the Safe Harbor Agreement. The ruling, which cannot be repealed, reflected the reasoning of Yves Bot, the advocate general of the Court, who said in a statement:

> *The law and practice of the United States allow the large-scale collection of the personal data of citizens of the E.U. which is transferred, without those citizens benefiting from effective judicial protection…Interference with fundamental rights is contrary to the principle of proportionality, in particular because the surveillance carried out by the United States intelligence services is mass, indiscriminate surveillance.*

So it was that the legal framework that facilitated the transfer of the PII of hundreds of millions of EU citizens to the U.S. companies was undone.

Within weeks, the European Commission clarified the ramifications of the Court's decision. The Article 29 Working Party—an organization created by the Data Protection Directive (Directive 95/46/EC) and composed of representatives from all EU Data Protection Authorities—noted that all transfers taking place under the aegis of the Safe Harbor Agreement are now "unlawful." It set a deadline of January 2016 for companies to demonstrate capabilities in keeping data localized, otherwise known as data sovereignty: "If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the

11 http://www.nationaljournal.com/s/64142/everything-we-learned-from-edward-snowden-2013

Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."[12]

The Article 29 Working Party did not go into specifics about these "coordinated enforcement actions," but observers could not help wondering if they would include the steep regulatory fines proposed by the European Parliament in its description of the new GDPR.[13]

The EU-U.S. Privacy Shield Agreement

January 2016 passed without any announcement of a joint solution. Then on February 2, the European Commission and the U.S. Department of Commerce announced a new agreement, the EU-U.S. Privacy Shield.

Designed to address the concerns the Court expressed in the Schrems decision, Privacy Shield promises to curtail mass surveillance of private individuals in the EU and to provide those individuals with legal recourse for the misuse of their data. "For the first time ever, the United States has given the EU binding assurances that the access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms," noted EU Commissioner Jourová.[14]

The new agreement includes these elements:

- **Strong obligations for companies handling Europeans' personal data and robust enforcement:** U.S. companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed. The Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under U.S. law by the US. Federal Trade Commission. In addition, any company handling human resources data from Europe has to commit to comply with decisions by European DPAs.

- **Clear safeguards and transparency obligations on U.S. government access:** For the first time, the U.S. has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be used only to the extent necessary and proportionate. The U.S. has ruled out indiscriminate mass surveillance on the personal data transferred to the U.S. under the new arrangement. To regularly monitor the functioning of the arrangement there will be an annual joint review, which will also include the issue of national security access. The European Commission and the U.S. Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European Data Protection Authorities to it.

- **Effective protection of EU citizens' rights with several redress possibilities:** Any citizen who considers that their data has been misused under the new arrangement will have several redress possibilities. Companies have deadlines to reply to complaints. European DPAs can refer complaints to the Department of Commerce and the Federal

12 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
13 http://www.computerweekly.com/opinion/EU-Data-Protection-Regulation-fines-up-to-100m-proposed
14 http://europa.eu/rapid/press-release_IP-16-216_en.htm

Trade Commission. In addition, Alternative Dispute resolution will be free of charge. For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.[15]

The Privacy Shield Agreement appears to address many of the concerns raised by Schrems, the ECJ, DPAs, and data privacy advocates. It introduces limitations to the data collection by U.S. intelligence agencies, and it ensures that the collection and use of PII is monitored. In addition, if EU citizens have complaints, they can take them to the Department of Commerce and the FTC, rather than to their local DPA, who might have less clout with U.S. companies.

Moving Forward: Beyond Safe Harbor and Waiting for Privacy Shield

Where does the announcement of Privacy Shield leave U.S. companies and third countries processing E.U. data?

Despite the sweeping language contained in the Privacy Shield announcement, no one is quite sure. Only the negotiators themselves know the particulars of the Privacy Shield Agreement. The Article 29 Working Party has requested that the European Commission provide documents describing the agreement's details within three weeks. The DPAs will then examine the agreement more closely and announce the findings of their legal analysis in April.

In the meantime, "DPAs are unable to draw conclusions about [Privacy Shield's] legality," according to Isabelle Falque-Perrotin, Chair of the Article 29 Working Party and President of the French National Commission on Computing and Liberty (CNIL).[16] The Working Party has issued a statement reminding companies that transfers to the U.S. on the basis of the original Safe Harbor Agreement remain invalid and that DPAs will continue to handle "related cases and complaints on a case-by-case basis."[17]

So it remains to be seen if the provisions in Privacy Shield will resolve the fundamental difference in perspectives between the EU, steadfast in asserting the right of its citizens to privacy, and the U.S. Government, steadfast in asserting the necessity of its intelligence agencies to collect whatever data they feel they need, which until recently meant collecting the private data of millions or—in the case of cell phones—billions of people.[18] [19] (Within U.S. intelligence agencies, these data collection operations have likely assumed a new urgency following the terrorist attacks in Paris and San Bernardino.)

Some companies, including Microsoft, had adopted Model Contracts instead of the Safe Harbor Agreement to manage data transfers for their cloud services. If these Model Contracts are found

15 http://europa.eu/rapid/press-release_IP-16-216_en.htm
16 http://www.csoonline.com/article/3029329/privacy/wait-until-april-before-relying-on-privacy-shield-eu-privacy-watchdogs-warn.html
17 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf
18 https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
19 19 At the same time that U.S. Commerce Dept. officials were negotiating Privacy Shield, Congress added the Cybersecurity Information Sharing Act (CISA) to an omnibus spending bill, which President Obama signed into law on December 18, 2015. To the chagrin of privacy advocates, CISA "allows companies to monitor users and share their information with the government without a warrant." http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/ Presumably, CISA allows companies and government agencies to monitor EU users. Under the terms of Privacy Shield, this activity would need to be vetted by both U.S. and EU officials.

not to prevent U.S. intelligence agencies from collecting PII "without limitation," they, too, could be deemed unlawful.

In fact, the Article 29 Working Committee's recent analysis of these contracts casts their legality in doubt, particularly because they fail to protect EU citizens from mass surveillance by the U.S.[20] BCRs may be questioned and struck down as well on the same grounds. As long as U.S. companies remain compelled to turn over high volumes of PII to U.S. intelligence agencies, no solid legal framework can exist for transferring EU PII to the U.S. or any other "third country" that shares data with the U.S.

Nevertheless, PII must be processed in order for multinational companies to continue to operate and engage in trans-Atlantic trade. But in order to process EU PII while avoiding enforcement actions, U.S. enterprises and other non-EU-based companies need to develop an alternative, compliant solution.

What strategies can these companies adopt for managing PII legally?

Strategies for Achieving Data Sovereignty and Compliance

Here are three strategies that U.S. companies and other enterprises can adopt to support compliance with EU data privacy regulations:

- Strategy #1: Audit internal PII practices.
- Strategy #2: Review content storage and distribution policies to ensure that EU data is kept within the EU.
- Strategy #3: Deploy private cloud data storage solutions to keep EU data local.

Let's examine each of these strategies in detail.

Strategy #1: Audit Your Organization's PII Practices

The first strategy is to audit PII practices. Enterprises should ask themselves:

- What data are we actually collecting?
- How is this data being stored?
- Where is it being stored? If it is being duplicated, where is the duplicate data being stored?
- Why are we storing so much data? Do we need all of it? Can some of the PII we have been collecting and storing be discarded?
- How long does the data really need to be kept?

20 http://www.csoonline.com/article/3029329/privacy/wait-until-april-before-relying-on-privacy-shield-eu-privacy-watchdogs-warn.html

Most large enterprises are unlikely to know the answers to these questions. A cross-functional team of IT, legal, and operations professionals will need to conduct a formal audit to get the answers.

Companies should begin this process right away. Without a thorough understanding of how much PII companies have and where it is stored, they will be unable to implement any sort of strategic or compliant solution for managing PII. An added benefit is that organizations may find that they can improve operational efficiencies and reduce data storage requirements (and therefore costs) by reducing the PII that they collect and minimizing the amount of time it is stored.

Strategy #2: Review Content Storage and Distribution Policies to Ensure EU Data Is Kept within the EU

Identifying which file servers and Enterprise Content Management (ECM) platforms such as Microsoft SharePoint are being used to store the PII of EU citizens is a good start, however it's only half the battle. Understanding how employees are sharing and distributing that information through email, file-sharing services such as Dropbox, chat tools, and other online services is an entirely different and more complicated matter. The same can be said for establishing and enforcing policies that regulate the sharing and distributing of data and PII.

Sharing content is an essential part of doing work, but it's far too easy today for employees to share content with unauthorized recipients, intentionally or unintentionally. The same lapses that can disclose confidential product plans through public cloud-based file-sharing services like Evernote[21] or customer records through email[22] can also lead to the disclosure of EU PII, triggering costly regulatory penalties.

After auditing their content collection and storage practices, enterprises should then audit their content sharing and distribution practices. If they discover that the business lacks any centralized monitoring of content sharing, they should begin evaluating content management solutions so that IT administrators and compliance officers can monitor and control the distribution of sensitive content, including the PII of EU citizens.

Strategy #3: Deploy Private Clouds to Keep EU Data Local

Enterprises in every industry are increasingly migrating IT services to the cloud to enhance performance, agility, and cost savings.[23] When adopting a cloud solution, many enterprises envision having to choose between public clouds for ease of adoption and low cost, and private clouds for control and security. On the contrary, private and hybrid clouds are proving to be as cost-effective as public clouds, once data security and data governance are factored into calculations. As a result, a growing number of enterprises now prefer private cloud and hybrid cloud options, especially for critical security applications such as content sharing.[24]

When it comes to data privacy, public cloud services pose serious risks. Many public cloud services were designed to meet the needs of consumers posting photos and personal files, rather than enterprises in regulated industries managing large volumes of sensitive content. These cloud storage providers have suffered security outages and often lack the monitoring and policy enforcement capabilities expected of more traditional enterprise software. In addition,

21 For example, see http://www.computerworld.com/article/2504460/byod/byod-exposes-the-perils-of-cloud-storage.html
22 http://www.eweek.com/c/a/Security/Email-Main-Source-of-Data-Leaks-in-Organizations-Survey-431836
23 In a 2014 survey, IDG found that 69% of enterprises had either applications or infrastructure running in the cloud, up from 12% in 2012. http://www.forbes.com/sites/louiscolumbus/2014/11/22/cloud-computing-adoption-continues-accelerating-in-the-enterprise/
24 http://www.accellion.com/blog/private-cloud-file-sharing-demand

many public cloud services were designed to move data automatically from data center to data center to optimize load balancing while minimizing operational expenses. While this strategy enhances storage and operational efficiency, it obscures the actual location of the data and puts it out of the customer's control.

To keep EU PII from U.S. intelligence and law enforcement agencies—and therefore compliant with new EU standards—a local storage solution is the best solution. It ensures enterprise customers know exactly where their data is stored, that the data is not co-mingled with another enterprise's data, and that the data is safeguarded using encryption keys solely owned and managed by the enterprise rather than the cloud provider. This last attribute is particularly compelling for an increasing number of enterprises as no user, provider, or government agency can decrypt content if the encryption keys are under the enterprise's full control.

EU regulators will hold enterprises, not their cloud service providers, ultimately responsible for any data breaches or compliance violations. Enterprises therefore need to select their cloud solutions carefully, ensuring that sensitive content such as the PII of EU citizens is carefully managed and secure.

kiteworks by Accellion

An Overview of the kiteworks Secure Content Platform

kiteworks is a Secure Content Platform from Accellion that empowers enterprises with secure content management and collaboration capabilities, while complying with strict data privacy regulations such as the Data Protection Directive. Specifically, the kiteworks platform offers enterprise organizations a secure file sharing and collaboration solution that enables secure internal and external sharing of enterprise information, and a development platform for designing and deploying custom enterprise applications to increase productivity, while ensuring data security and compliance.

Key features of the kiteworks platform include:

- Enterprise-grade secure file sharing and collaboration capabilities
- Widest choice of deployment options, including a 100% on-premises private cloud
- Secure access to enterprise and cloud content sources – without requiring a VPN
- Comprehensive file tracking and reporting for IT management, control, and compliance
- Integration with existing enterprise IT security systems, including AD/LDAP, DLP, SSO, MDM, and SFTP
- Secure mobile container with integrated editor, encryption, and remote wipe
- Mobile SDKs for iOS, Android, and Google Glass
- Enterprise APIs to integrate with and extend existing enterprise infrastructure to mobile

The Advantages of a Tiered Architecture

Critical for compliance with EU data privacy regulations, the kiteworks platform features a flexible

tiered architecture that enables Web, application, and data storage tiers to be deployed and scaled separately as needed. Any or all tiers may be deployed as private cloud services, giving enterprises full control over the security and location of their data.

The diagram below depicts these tiers, which are included whether the platform is deployed as a virtual appliance or on physical servers in a data center or a cloud service.

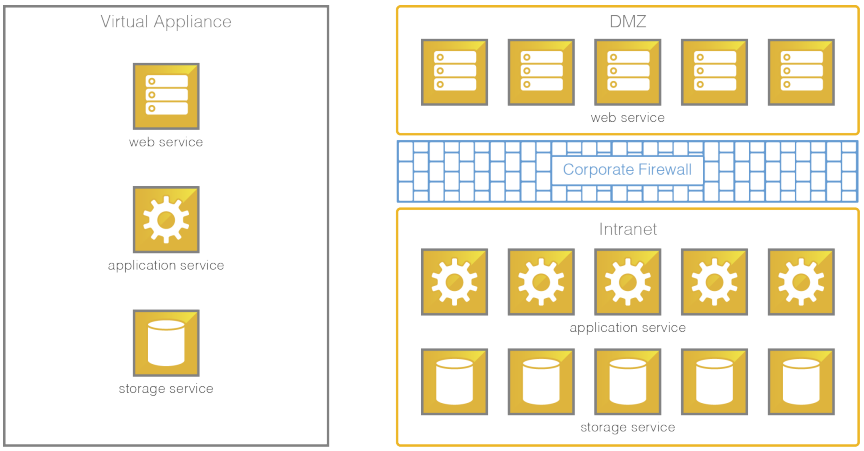

Figure 1: The three-tier architecture of the kiteworks platform supports flexible deployments while eliminating a single point of failure.

Replicating the three tiers in North America and the EU enables a global organization to deploy a single solution that meets the data privacy and data sovereignty requirements of the EU.

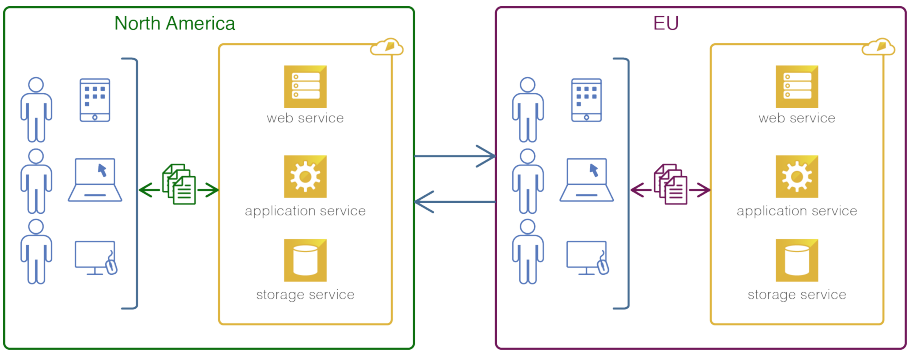

Figure 2: Deploying separate instances of kiteworks in North America and the EU provides a consistent experience for employees in both regions while complying with EU data privacy regulations.

The kiteworks solution can be used by global enterprises as well as by enterprises with offices only in the EU.

In addition, the solution can be deployed:

- 100% on premises
- 100% in a private hosted cloud
- Mixed in a hybrid cloud combining on-premises services with private hosted cloud services for greater scalability

The following scenarios show how enterprises can use kiteworks to provide employees with powerful, secure, and easy-to-use content sharing and distribution services while meeting data privacy regulations in all locations where they have offices.

Scenario #1: Global Enterprise with Services 100% On-Premises

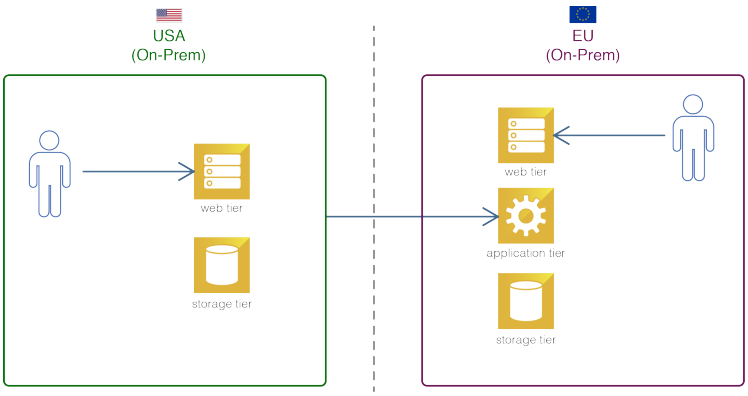

Figure 3: A kiteworks solution for a global enterprise with offices in the U.S. and the EU.

In this scenario, users in both the U.S. and the EU are able to access a local Web storage tier. Application logic, including data sovereignty rules, is hosted in the EU, and directs users in each region to their local data storage services.

Scenario #2: Global Enterprise with Hybrid Cloud

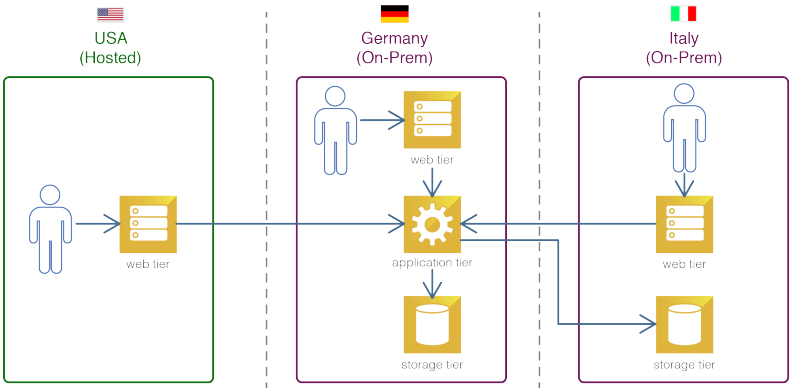

Figure 4: A hybrid cloud enables an enterprise to combine on-premises services with private hosted cloud services to meet goals for both performance and compliance.

Some enterprises may decide they do not need to deploy storage tiers on premises in every region. In the example above, only the Web tier is deployed in the U.S.

All users access an application tier hosted in whatever country has the strictest data privacy laws; in the example above, the application tier is hosted in Germany. Data sovereignty policies in the kiteworks platform automatically direct users to the storage tier appropriate for their location. For users in the US and Germany, the storage tier resides in an on-premises facility in Germany. For users in Italy, the storage tier resides in an on-premises facility in Italy.

This custom architecture offers several benefits:

- Compliance with data privacy regulations
- High performance through local Web access
- Cost savings from limited duplication—the enterprise is spared the expense of duplicate application tiers in the U.S. and Italy and the expense of data storage in the U.S.

Scenario #3: EU Enterprise with Services 100% On Premises

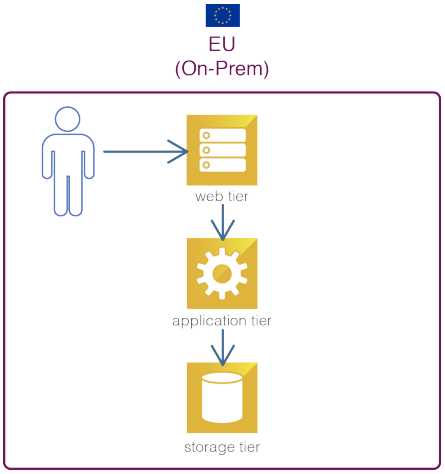

Figure 5: An on-premises solution in the EU keeps all data and services local.

An enterprise based in the EU has the option of deploying all three kiteworks tiers on premises and fully under local control. Since all services are running locally, the enterprise can easily comply with the Data Protection Directive and any other relevant data privacy regulations.

Scenario #4: EU Enterprise with 100% Hosted Solution

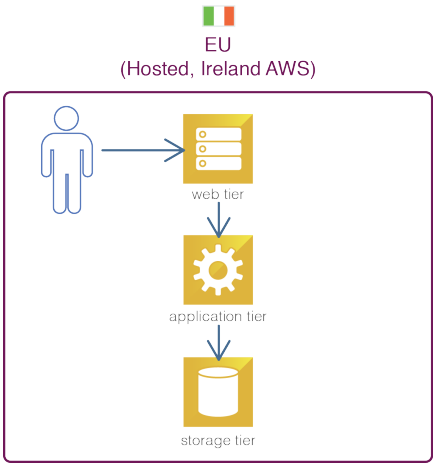

Figure 6: An EU enterprise can optionally deploy kiteworks in a private hosted cloud, such as a private cloud running on Amazon AWS in Ireland.

If the cost savings of a private hosted solution appeal to an EU enterprise, all three tiers may be deployed in a private hosted cloud. This solution provides the flexibility and cost savings of a cloud deployment, while avoiding the security and compliance risks of public cloud services.

Scenario #5: EU Enterprise with a Hybrid Cloud

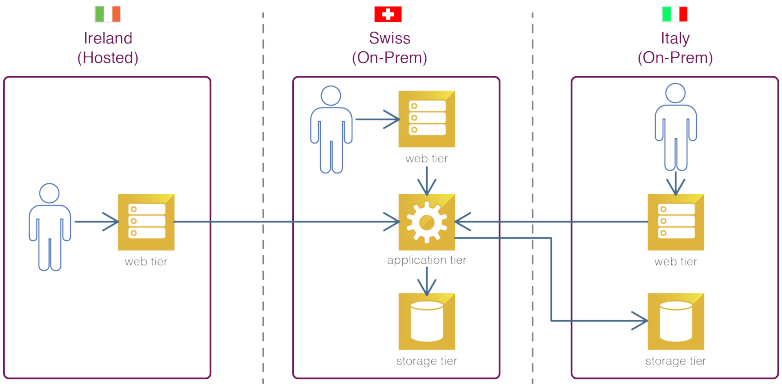

Figure 7: A hybrid cloud enables an enterprise with operations only in the EU to combine hosted services with on-premises services to meet goals for both performance and compliance.

Finally, an enterprise based wholly in the EU can adopt a hybrid cloud, just as a global enterprise can (see scenario #2). Users access locally hosted Web tiers, which route requests to an application tier hosted in whatever country has the strictest data privacy laws; in this example, the tier is running on premises in Switzerland. Data sovereignty policies in the kiteworks platform automatically direct users to the storage tier relevant for their location.

Other Benefits of the kiteworks Solution

In addition to helping enterprises comply with the EU Data Protection Directive and similar data privacy regulations, the kiteworks platform offers other benefits for enterprises, regardless of where they are located.

For example, the kiteworks platform enables secure access, editing and sharing of enterprise content on any type of device. Users have access to all content stored across the enterprise from a single pane of glass, enhancing employee productivity, content security and regulatory compliance.

The kiteworks solution has earned Accellion a position in the Gartner Magic Quadrant “Leaders” Quadrant for Enterprise File Sync and Sharing. Accellion has over 2,000 enterprise deployments, over 14 million enterprise users, and a customer renewal rate of 110%. Its customers range from leading corporations such as Proctor & Gamble, Pfizer and Verizon to universities such as Harvard University and Rutgers to government agencies such as NASA, NIST, the Securities and Exchange Commission, and the UK NHS.[25]

Conclusion

The European Court of Justice’s decision is irrevocable: the Safe Harbor Agreement that facilitated the legal transfer of EU data to the U.S. and other third countries is now void. While government agencies and lawmakers assess the new Privacy Shield agreement, enterprises cannot afford to stand still. Enterprises on either side of the Atlantic should seek solutions that directly manage and protect the PII of EU citizens. At the same time, they should evaluate their internal content management practices and strategies and look for opportunities for optimizing their content collection, storage, and management capabilities.

The kiteworks platform by Accellion offers enterprises a powerful, secure, and flexible solution for implementing compliant content management solutions, regardless of an organization’s geographic distribution or nation of origin. By adopting kiteworks, enterprises can keep control over PII and other sensitive data, while benefiting from a flexible, multi-tier architecture that can adapt to changing business needs as well as changing laws and regulations.

For more information about Accellion’s kiteworks secure content platform, please visit www.accellion.com.

25 For a longer customer list, visit http://www.accellion.com/about-us/our-customers.

Glossary

Article 29 Working Party
Officially, "Working party on the Protection of Individuals with regard to the Processing of Personal Data," an organization created by the Data Protection Directive (Directive 95/46/EC), is composed of representatives from all EU Data Protection Authorities, the European Data Protection Supervisor (EDPS), and the European Commission. It has advisory status and acts independently.

Data Controller
A person or organization collecting, storing, and managing the personal data of a private citizen.

Data Localization
The principle that data regarding the private citizens of a nation should be stored within that nation.

Data Privacy
Preserving the confidentiality and integrity of data, especially data involving private citizens or containing confidential material such as product designs.

Data Protection Authority (DPA)
The government agency in an EU Member State responsible for enforcing EU data privacy regulations.

Data Protection Directive
The European Union's directive (Directive 95/46/EC) that established the right of private citizens of EU countries to know who is collecting their data, to know how that data is being used, and to withdraw their data from future use at any time.

Data Sovereignty
The principle that data stored in a country is subject to the laws and regulations of that country.

Data Subject
A private citizen whose data is being processed by a data controller.

General Data Protection Regulation (GDPR)
A new data privacy directive proposed by the European Commission in 2012 to update the earlier directive to account for social networks and cloud services. The new regulation should broaden the scope of data privacy rules to cover any organization with private data about EU citizens. A single set of rules would apply to all EU members. Fines for non-compliance could reach up to €1 million or up to 5% of global revenue, whichever is higher.

Personally Identifiable Information (PII)
Data that can be used to identify a specific person.

Privacy Shield
A new EU-U.S. privacy agreement that replaces Safe Harbor and promises to end mass surveillance of EU citizens' data while requiring U.S. companies to comply with EU data privacy regulations.

Private Cloud
A cloud computing service that is run either in an organization's internal data center or in a private, dedicated hosting center fully under the control of the organization.

Safe Harbor Agreement
An agreement negotiated by U.S. and the European Union allowing the PII of EU citizens to be exported to U.S. companies if those companies certified that they were adhering to the principals of the Data Protection Directive.

Email: sales@accellion.com
Phone: +1 650 485 4300

Accellion, Inc.
1804 Embarcadero Road
Palo Alto, CA 94303