ALBRIGHT STONEBRIDGE GROUP

SAFE HARBOR AND THE PATH FORWARD

NOVEMBER, 2015

SUMMARY

- In the wake of the European Court of Justice (ECJ) ruling to invalidate the Safe Harbor agreement -- which for 15 years has permitted the free flow of information across the Atlantic – businesses face an atmosphere of continued uncertainty. Companies have until January 2016 to ensure compliance with data protection requirements, and have limited and potentially costly options going forward.

- National data protection authorities (DPAs) have been given additional authority to investigate and enforce national privacy laws. In the absence of Safe Harbor, companies should be prepared to engage each of these authorities individually.

- European Justice Commissioner Věra Jourová visited the United States in mid-November to address the final sticking points to an agreement. Commissioner Jourová previously stated that an agreement had been reached "in principal," and expects to conclude negotiations with the U.S. Department of Commerce by the end of 2015.

- While negotiators have made significant progress toward reaching a new arrangement, there is no assurance that it will survive ECJ scrutiny. Companies should be prepared to operate in an extended period of uncertainty in the coming months.

- A new agreement is likely to focus on transparency and accountability mechanisms for U.S. agencies that use European data for national security purposes. If an agreement is dependent upon U.S. legislative action, it is unlikely to be finalized by the January deadline.

ABOUT ASG

Albright Stonebridge Group (ASG) is a leading global strategic advisory firm that helps our clients succeed by assessing and managing risks, identifying and seizing opportunities, and solving commercial, political, and regulatory challenges in international markets.

Chaired by former U.S. Secretary of State Madeleine K. Albright, White House National Security Advisor Samuel R. Berger, and Secretary of Commerce and Kellogg Company CEO Carlos M. Gutierrez, ASG's worldwide team of commercial diplomats has served clients in more than 100 countries and across all major industries.

ALBRIGHTSTONEBRIDGE.COM

CONTEXT

On October 6, 2015, the European Court of Justice (ECJ) invalidated the so-called "Safe Harbor" agreement -- which for the past 15 years -- permitted information of European citizens to be stored on servers in the United States. Current EU data protection regulations require the "essential equivalence" of regulations for any non-EU country where personal information is stored. Eleven countries meet such a standard, and only through additional assurances that companies agreed to under Safe Harbor were they permitted to store information on U.S. soil. It was considered crucial to the operation of U.S. - based technology companies, from small and medium enterprises to major internet companies such as Google and Facebook.

The ruling occurs within a broader effort in Europe to re-inforce data protection as a fundamental right of European citizens. The European Commission is expected to act on two key proposals in the coming months. First, by the end of 2015, the Commission is expected to finalize an updated EU Data Protection Directive. This directive is intended to expand the jurisdiction of European authorities, and to hold any company that provides services in Europe to the same privacy standards. Second, the EU Digital Single Market strategy, which seeks to harmonize regulations across the region, will require the 28 member states member states to agree on a single framework for data protection. This has the potential to both reduce bureaucratic red tape, and lead to cumbersome privacy regulations for the entire region.

The Safe Harbor case can be traced to the 2013 revelations of Edward Snowden, who exposed U.S. National Security Agency (NSA) programs to collect information on foreign citizens that flowed through data centers in the United States. A complaint to the European Court of Justice by Austrian privacy advocate Max Schrems focused on the inability of Safe Harbor to adequately protect his personal information from "indiscriminate" surveillance from the NSA. The ECJ ultimately agreed with Schrems, stating that because Safe Harbor protections were subordinate to national security and law enforcement interests, they were not adequate to protect European citizens.

In the absence of Safe Harbor, uncertainty has prevailed, and is likely to continue as negotiators on both sides of the Atlantic search for a path forward. The Article 29 Working Party, which represents each of the 28 national data protection authorities (DPA) in the European Commission, set an enforcement deadline of January 31, 2016. By that time, more than 4,000 companies that previously relied on Safe Harbor must find new mechanisms to comply with EU regulations or face investigation and possible fines.

OPTIONS FOR COMPANIES

There are two primary mechanisms for businesses to maintain compliance with EU data protection regulations, each with its own challenges.

The first are so-called "Binding Corporate Rules" (BCRs), which are a set of regulator-audited and approved internal assurances to protect user data. Binding Corporate Rules are the safest option available for companies, but can be costly and time-consuming to implement. BCRs are comprehensive internal arrangements that dictate how user data may be transferred within the company and across subcontractors to ensure adequate protection. They require the long-term involvement from senior

leadership, careful coordination with contractors, and development of internal codes of conduct to ensure transparency and accountability regarding the use of user data. BCRs sometimes take more than 9 months to develop, and given the regulatory and legal expenses, BCRs may not be a viable route for small and medium-sized companies.

The second option for businesses are known as "Standard Contract Clauses" (SCCs), which are a set of standard contracts developed by the European Commission. These contracts are used as an assurance of proper data protection when information is transferred outside of Europe, even when information is contained within the same company but transferred to another location. A contract must be agreed to for each instance that data is transferred, and may not be practical for companies managing continuous data transfers across the Atlantic.

Both BCRs and SCCs are highly vulnerable to legal challenge in the wake of the Safe Harbor decision because companies cannot guarantee that their users will be protected from foreign surveillance or law enforcement investigations. In Germany, for example, the Schleswig-Holstein State indicated skepticism that current protections under SCCs would be sufficient in the absence of broader reforms by the United States. While the European Commission has fiercely defended BCRs and SCCs, German data protection authorities are expected to meet in the coming weeks to discuss their use for German citizen data.

The possible challenge to BCRs and SCCs has raised fears that companies may be forced to store all European user data on servers located within EU boundaries. Some companies have already considered this approach, indicating a willingness to redesign their infrastructure despite the additional cost because they require certainty for continued operation. The most significant company to move in this direction is Microsoft, which announced that it plans to give European customers the option to store personal data on servers located in Germany – likely in an effort to appease the region's most concerned data protection agencies.

The move by Microsoft added to concerns of data localization in Europe, which would have significant economic and political consequences in the region, and could be devastating for small and medium-sized companies.

Possible Paths Forward

Negotiators from the U.S. and the EU have moved quickly to revive talks for a new agreement that will survive in the post-Snowden era. On October 26, EU Justice Commissioner Věra Jourová announced that a framework had been agreed upon "in principal" by both sides. A few days later, U.S. Secretary of Commerce Penny Pritzker confirmed Commissioner Jourová's statement saying that a "solution is within hand." This new agreement relies on increased transparency and specific notification of European authorities when European data is used in national security or law enforcement investigations.

While this announcement is a sign of progress, optimism that business will resume as usual for technology companies in Europe should be tempered. A framework will require successful negotiations not only between the European Commission and the U.S. Department of Commerce, but also between the national data protection authorities and the Commission itself. In addition, a new arrangement that will satisfy ECJ scrutiny will depend on enhanced trust, transparency, and accountability between Europe, multinational

companies, and the United States government. It will be a high bar to clear, and there are several challenges to ensure a proper mechanism for the efficient flow of information across the Atlantic.

Given these challenges, there are several possible outcomes to the ongoing negotiations. The most likely scenario will include continued uncertainty even if an agreement is reached by U.S. Department of Commerce and EU Justice Commission officials.

Scenario 1: New arrangement reached

An agreement that would replace the Safe Harbor framework with a new, central set of compliance mechanisms for companies would be the best-case scenario for multinational businesses. Ultimately, the United States will need to convince Europe that sufficient reforms have been made to U.S. surveillance programs since Snowden's 2013 revelations. U.S. Department of Commerce officials, who are negotiating the Safe Harbor agreement, and Federal Trade Commission officials, who have oversight over data protection issues in the U.S., will make the case that President Obama has taken action to increase oversight and transparency of the NSA. While modest progress has been made, European officials will likely demand additional concessions.

The complicating factor in the negotiations is that any new agreement between the EU Commission and the U.S. Department of Commerce would require the affirmation of other institutions. In addition to the Commission, the European Parliament and the data protection agencies would need to approve a new agreement – which may be tied to additional concession by the United States and require U.S. Congressional action. At any point during deliberations in Parliament, an ECJ review of a new agreement could also be requested, adding further pressure to the negotiators.

The agreement announced by Commissioner Jourová is likely to focus on enhanced transparency by requiring U.S. authorities to notify European officials when information is used for national security or law enforcement investigations. However, it may also be tied to enhanced accountability measures. This would likely require U.S. Congressional action – such as the Judicial Redress Act of 2015 – that would allow European citizens to sue the U.S. government if their information is misused. The Judicial Redress Act is currently being considered by the Senate, after passing in the House of Representatives on October 20.

Scenario 2: Delay and uncertainty

Given the current political environment, a prolonged period of uncertainty as negotiations drag past current deadlines is possible.

Recent developments on both sides of the Atlantic do not bode well for compromise. On October 27, Congress passed the Cybersecurity Information Sharing Act (CISA), further inflaming concerns that the U.S. government would obtain personal user information in coordination with technology companies – a primary concern of the Safe Harbor case. In Europe, meanwhile, the parliament passed a resolution to

recognize Edward Snowden as a "whistle-blower and international human rights defender.[1]" While it did not include a commitment to grant Snowden asylum, the resolution encouraged his protection from U.S. prosecution. These recent developments do not bode well for an atmosphere of compromise on both sides – and make an easy resolution more difficult.

Under pressure from the United States and European Commission officials, it is possible that the organization of European data protection officers – the so-called Article 29 Working Party -- may decide to extend the current January enforcement deadline. This would give companies breathing room as they move forward with alternative compliance mechanisms, but not more clarity on a long-term solution. How much time national data protection authorities will give European negotiators remains to be seen, as they too may begin to face pressure from citizens, and countries such as Germany or France who may be more eager to see action against companies perceived to be complicit in foreign surveillance.

Scenario 3: Compliance, at a cost

In a worst-case scenario, any agreement to replace Safe Harbor could be immediately challenged and invalidated by the European Court of Justice. Companies would then need to rely upon BCRs and SCCs as a permanent compliance solution – unless those too are challenged by data protection authorities. While transatlantic data flows may continue in the interim, some companies may be forced to operate in a questionable legal environment – and large companies are likely at a higher risk for early investigatory action.

While current compliance issues faced by companies are limited to U.S. – EU data flows, the ruling could have an impact on data transfers to other countries as well. Europeans have even called into question data protection issues of fellow EU member countries. In particular, they have criticizes the mass surveillance programs in the UK and France. If the data protections of European countries are challenged, it could threaten the larger European goal of creating a single digital market in Europe, and make technical operations in the region difficult.

In a truly worst-case scenario, these continued challenges to data protection regimes could force companies to simply localize data in the region. For more information on economic and political consequences of data localization, see Albright Stonebridge Group's September 2015 report here.

[1] European Parliament Press Release. "Mass Surveillance: EU citizens' rights still in danger, Parliament says". October 29, 2015.
http://www.europarl.europa.eu/pdfs/news/expert/infopress/20151022IPR98818/20151022IPR98818_en.pdf