Foreword

According to the website Europe v Facebook, Ireland’s Data Protection Commissioner is planning to refer the Facebook case back to the Court of Justice of the European Union (CJEU) to determine if Facebook can continue to transfer data from the European Union to the United States by using EU model clauses.

In the Maximillian Schrems v Data Protection Commissioner case of 2015, the CJEU invalidated the “Safe Harbor” framework system, which was used by numerous companies to transfer data from the European Union to the United States. According to the Safe Harbor website, over 4,000 companies were registered under the program. As a result of the CJEU decision, a number of companies decided to rely instead on other transfer mechanisms, such as Standard Contractual Clauses and Binding Corporate Rules. However, are these mechanisms truly full-proof?

In our February newsletter, we wrote that the CJEU’s holding in the Schrems case is that any international pact or agreement, or even a decision from the EU Commission, would not prevent a DPA from assessing whether an adequate level of protection really exists in relation to a transfer of personal data to any country or territory outside the EEA (line 66 of the CJEU ruling). Thus, any framework for the transfer of personal data outside the EEA could be invalidated.

It appears that the Irish authorities will put this to the test, since according to the website Europe v Facebook, the Irish Data Protection Commissioner will refer a case to the CJEU for it to determine if Facebook may transfer data from the EU to the US by using the EU model clauses.

With the uncertainty surrounding the future of the new "Privacy Shield" (see article below - "EU Data Protection Supervisor voices concerns over Privacy Shield"), it seems that uncertainty is set to become the new normal for international companies transferring data from the EU to the US.

We hope that you enjoy reading this newsletter as much as we enjoyed preparing it. Please do not hesitate to contact us about any ideas you
Paul Lanois

EU and US sign "Umbrella agreement"

On 2 June 2016, the European Union and the United States of America signed the so-called "Umbrella agreement" which puts in place a high-level data protection framework for criminal law enforcement cooperation. The agreement is meant, among others, to improve EU citizens' rights by providing equal treatment with US citizens when it comes to judicial redress rights before US courts.

The "Umbrella agreement" covers all personal data exchanged between police and criminal justice authorities of the EU member states and the US federal authorities for the purpose of prevention, investigation, detection and prosecution of criminal offences, including terrorism.

The agreement is meant to facilitate criminal law enforcement cooperation while, at the same time, providing safeguards and guarantees of the legality of data transfers. Those include, for example, provisions on clear limitations on data use, the obligation to seek prior consent before any onward transfer of data, the obligation to define appropriate retention periods, the right to access and rectification, etc.

The agreement is further meant to complement existing and future EU-US and member state-US agreements between law enforcement authorities. The press release states that the agreement is not in itself a legal instrument for any transfer of personal information to the US but it supplements, where necessary, data protection safeguards in existing and future data transfer agreements or national provisions authorising such transfers.

Source:
EU Press Release - Enhanced data protection rights for EU citizens in law enforcement cooperation : EU and US sign

EU Data Protection Supervisor voices concerns over Privacy Shield

Criticism on the Privacy Shield continues to pile on. In April, national data protection authorities from across the EU expressed significant concerns over the Privacy Shield framework.

In May, the European Parliament voiced their concerns about "deficiencies" in the Privacy Shield, notably:
- the possibility of collecting bulk data, in some cases, which does not meet the criteria of "necessity" and "proportionality" laid down in the EU Charter of Fundamental Rights;
- the proposed US ombudsperson, who would not be "sufficiently
independent” nor “vested with adequate powers to effectively exercise and enforce its duty” according to the MEPs; and
- the complexity of the redress mechanism, which the Commission and US administration need to make more "user-friendly and effective", according to the MEPs.

Now it's the turn of the European data protection supervisor, appointed by the Commission to advise EU institutions on privacy and data protection matters, to voice his concerns.

Giovanni Buttarelli, EDPS, said: "I appreciate the efforts made to develop a solution to replace Safe Harbour but the Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court. Significant improvements are needed should the European Commission wish to adopt an adequacy decision, to respect the essence of key data protection principles with particular regard to necessity, proportionality and redress mechanisms. Moreover, it's time to develop a longer term solution in the transatlantic dialogue."

Source:
EDPS Press Release - Privacy Shield: more robust and sustainable solution needed

**German DPAs demanding more staff and resources**

The conference of the independent German data protection authorities ("conference"), in a resolution of 25 May 2016 (German), calls on the German legislator to provide the data protection authorities with more staff and financial resources so they can effectively meet their assigned duties.

The German authorities refer to article 52 paragraph 4 of the GDPR, which states that: "Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the [future European data protection] Board."

Once the GDPR is fully applicable, this provision could represent a new challenge for some EU member states since the European Commission may sue a member state by means of an infringement proceeding under article 258 of the Treaty on the Functioning of the European Union (TFEU). Carlo Piltz notes that such an infringement action was already brought before the Court of Justice of the European Union under the current data protection directive in Case C-614/10.
Google challenges French fine on "right to be forgotten"

Since the Court of Justice of the European Union (CJEU) handed down its decision on May 13, 2014 on the "right to be forgotten", Internet users residing in Europe can, under certain conditions, ask search engines to delist information about them. Should a search engine refuse to delist search results or respond unsatisfactorily, Internet users residing in Europe may take the matter to their national data protection authority. In 2015, the French data protection authority, the CNIL, took a very broad approach, stating that the delisting should apply to searches on all Google properties worldwide, not just to EU domains.

In March 2016, the CNIL issued a €100,000 fine against Google for failing to implement a global delisting. Google has recently announced that it has filed an appeal of the CNIL’s order with the French Supreme Administrative Court, the Conseil d’Etat.

Read more:

Google Europe Blog - A principle that should not be forgotten

Future events

HIPAA, Privacy and Security Fundamentals

The news in 2015 was filled with high profile data breaches of healthcare information. As the use and exchange of healthcare information continues to increase, understanding the fundamental compliance requirements under the HIPAA Privacy, Security, and Enforcement Rules and under the HITECH Act is critical for attorneys and professionals who are advising entities that handle "Protected Health Information."

This HIPAA Fundamentals program is a webinar you need to attend if:
- You're a newly licensed attorney working in the healthcare industry
- You're no longer considered "newly licensed," but occasionally have to answer a HIPAA-related question
- You're a business associate to a covered entity
- You think you might be a business associate
- You work in an information technology capacity in the healthcare industry and you occasionally or routinely access and/or update patient information or help others in your organization to do so
You work in a healthcare compliance position, whether for a hospital, physician's office, or insurance company.
- You are a litigator and issue subpoenas for or routinely review health information records in your cases.
- You are in-house counsel at a healthcare entity.

Topics that are covered in this webinar, as well as what attendees should expect to learn, include:
- A refresher on the HIPAA's and the HITECH Act's basic requirements.
- An overview of the HIPAA Privacy Rule.
- A detailed description of business associates and their roles and requirements.
- A summary of the HIPAA Security Standards.
- An in-depth examination of the data breach notification standards and requirements.
- A discussion of recent HIPAA enforcement activity.

**Format:** Webinar

**Date:** June 16, 2016

**Time:** 12:00 PM - 1:30 PM ET

**Credits:** 1.50 General CLE Credit Hours

**Panelist(s):** Kimberly J Gold and Richard Marotti

**Moderator:** Peter D Ricoy

Register here for the HIPAA, Privacy and Security Fundamentals webinar.