After Safe Harbor:
Navigating Unknown Data Privacy Waters

LLM LIQUID LITIGATION MANAGEMENT, INC. | Logical Solution. Legendary Service.

What began as a data privacy case against Facebook in Ireland resulted in the Court of Justice of the European Union (CJEU) ruling that Safe Harbor was no longer valid. When the CJEU handed down its decision invalidating the 15-year-old international agreement between the United States and European Union, it set off waves of anxiety and uncertainty: Among other issues, just what did it mean for litigation and e-discovery data transfers?

This article will explore how Safe Harbor managed to fail the CJEU's test to begin with, ongoing efforts to resolve the gap between the EU and the United States on data protection, including the recent EU-U.S. Data Privacy Shield agreement, recommended best practices for e-discovery and more.

The CJEU's final ruling on October 6, 2015, invalidated the Safe Harbor framework.

IT STARTED WITH SCHREMS

In 2013, Max Schrems, an Austrian Ph.D. student, privacy advocate and Facebook user since 2008, filed a complaint with the Irish Data Protection Commissioner. He alleged that as a result of the mass National Security Administration (NSA) surveillance that Edward Snowden, a former contractor for the U.S. government, had revealed that year, adequate protections to the data he supplied to Facebook, some or all of which was then transferred from Facebook's Irish subsidiary to U.S.-based servers, could not be provided under the Safe Harbor framework. The Irish Data Protection Commissioner rejected the complaint, referencing the protection offered by the Safe Harbor framework. Schrems appealed the decision before the Irish High Court, which eventually referred questions to the CJEU. The CJEU's final ruling on October 6, 2015, invalidated the Safe Harbor framework.[1]

It's important for organizations to identify whether they're already following data transfer and data protection best practices.

BUT WHAT DOES IT MEAN?

Since the U.S.-EU Safe Harbor framework was approved in 2000 after the European Commission's Directive 95/46/EC (the Directive) was adopted in 1995, personal data has been allowed to freely move between the European Economic Area (EEA) and organizations in the United States who had self-certified that they will follow the Safe Harbor framework.

The invalidation of the Safe Harbor framework affects anyone — outside of law enforcement agencies in EU member states — looking to transfer data from the EEA to the United States. It's important for organizations to identify whether they're already following data transfer and data protection best practices. At the same time, companies should track both the activity of individual data protection agencies in EU member states to clarify the limbo and track the progress of changes to the framework. These decisions could potentially cost international organizations working with consumer data significant sums of money as they move to meet the needs of performing their business on an international field . For example, the price will be high for those organizations implementing application design changes that promote privacy or infrastructure changes focused within the EU.

In some European jurisdictions, corporate data transfers are already being challenged. For example, Germany appears to be pushing for a zero-transfer policy while we wait for a suitable Safe Harbor replacement to be agreed upon. In fall 2015, Johannes Caspar, Hamburg's Commissioner for Data Protection and Freedom of Information, said, "Anyone who wants to escape the legal and political implications of the CJEU judgment should in [the] future consider storing personal data only on servers within the EU."[2] They intend to investigate any post-Safe Harbor data transfers, specifically targeting companies like Google and Facebook. If more data protection authorities adopt Caspar's view on data transfer, it could mean more than additional IT infrastructure costs. In fact, if Caspar has his way, international organizations' German offices may be forced to act as standalone business units. Recently, Caspar expressed

his belief that when the individual Data Protection Authorities (DPAs) consider in April whether a proposed replacement to Safe Harbor will provide sufficient protection they will not find it adequate . If such is the case, companies will likely be given time to become compliant with personal data transfer, such as infrastructure changes or implementing one of the remaining legal options, Standard Contractual Clauses (Model Clauses) or Binding Corporate Rules.[3]

One of the glaring issues with the old Safe Harbor framework was the lack of oversight.

In other jurisdictions, organizations that wish to transfer data from the EEA are left to decide if their respective situation meets any of the exemptions outlined in Article 26(1) of the Directive.

Recently, Facebook became one of the first to face action. France announced the company has three months to stop tracking non-users' activities after the Safe Harbor deadline passed.[4] Facebook announced that it has alternative legal structures in place to Safe Harbor in conjunction with EU law. It's important that companies ensure that proper documentation and protocols for solutions are maintained and followed in order to avoid enforcement actions.

ONGOING EFFORTS

Fortunately, data protection authorities in the EU and United States are clearly working to lift everyone from this post-Schrems limbo.

One of the glaring issues with the old Safe Harbor framework was the lack of oversight. Organizations were self-certified and — short of investigations into potential violations of the Directive by data protection authorities — there were no audits. This meant there was no guarantee that organizations transferring data under Safe Harbor would adhere to the data protection principles. Safe Harbor also lacked an official means of redress for data subjects who felt their data was mishandled by an organization transferring data to third-party countries, especially in cases where that data was subject to law enforcement agency collection as part of mass surveillance efforts.

With the recent passage of H.R. 1428, the Judicial Redress Act, the United States has made a step in the right direction to remedy the issues that were ultimately part of the downfall of Safe Harbor.[5] The legislation offers protection for "citizens of certified states" by giving them the ability to bring civil action and obtain civil remedies in the same manner as well as to the extent they would in their respective "covered country." While this doesn't resolve all of the issues at hand, it does provide a legal foothold for data subjects who feel their data has been mishandled. As part of the EU-U.S. Data Privacy Shield agreement, the proposed replacement for Safe Harbor, an ombudsman will be appointed to address complaints passed on by member states' data protection authorities.[6]

In the "Safe Harbor 2.0" agreement, which is expected to be finalized for review around the end of February 2016, new protections will be introduced that include additional oversight and regular audits.[7] While this seems like it could put an end to the wait for a Safe Harbor replacement, it has yet to pass the test of the CJEU — and there is a very real possibility that it won't. Both the Judicial Redress Act and the Data Privacy Shield agreement have provisions for mass surveillance — arguably the primary cause for the fall of Safe Harbor.

BEST PRACTICES FOR E-DISCOVERY

When the EU first adopted the Directive in 1995 as a means to protect the privacy and personal data of its citizens, it required that seven specific principles be followed.

- **Notice**: Data subjects must be made aware of any data processing/collection.
- **Purpose**: Targeted data should be collected in accordance with the purpose given to the data subject when notified of collection effort.
- **Consent**: The data subject must consent to the processing and transfer of personal data.
- **Security**: Adequate security must be offered for any and all personal data that was collected.
- **Disclosure**: The data subject must be informed as to the parties involved with collection/processing of their personal data.
- **Access**: Collected data should be made available to the data subject for review, should any data require correction.
- **Accountability**: Parties involved in collection and processing of data should be held accountable for any violations of these principals, should the data subject decide their data was mishandled in any way.

Therefore, when an organization transferred personal data under Safe Harbor, they were doing so under the assumption that these principles would be followed. In many ways, however, the principles were not followed by all — Safe Harbor certification or not.

In many ways, however, the principles were not followed by all — Safe Harbor certification or not.

Moving forward, organizations that did self-certify but didn't properly implement the framework's protocols will have to change. By contrast, those that did self-certify and also followed the Safe Harbor framework and principles of the Directive will enjoy a strong foundation for the alternatives options that are currently available and to any upcoming changes to data transfers with the EU.

Several options remain available to properly handle data transfers including those of the e-discovery variety. At their core, each of these methods answers the core concerns of data protection by asking the right questions:

- Do we know what is being collected and why it is being targeted?
- Have we limited the scope as much as possible to avoid bringing in irrelevant information (potential PII)?
- Do we know what protections we have in place to ensure the PII is safe?
- Do we have a means of returning all information should the custodian decide he or she no longer wishes to cooperate?
- Have custodians been given notice about how their data will be used?

Perhaps, the easiest option is gaining the data subject's consent in writing, per Article 26(1)(a) of the Directive. The Article 29 Working Party has put together very clear guidelines on gaining proper consent. The data subject's consent must be freely given, specific, unambiguous, explicit, informed and not coerced in any way.[8] Thorough documentation should be maintained to prove the consent meets these criteria as well as others provided by the Article 29 Working Party. When consent is provided, data may then be processed/transferred in accordance with the notice that was clearly provided to the data subject when requesting his or her consent. If, for any reason, the purpose of the collection/processing/transfer of the data should change, consent must be gained again to cover the new use of the data.

MODEL CONTRACTS

Another option for properly handling data transfer is to have an agreement in place containing the standard contractual clauses (or "Model contract clauses") as approved

by the Commission — Article 26(2) of the Directive — and recommended as an alternative by the European Commission after the CJEU Safe Harbor decision.[9]

Model contract clauses are available for two specific uses: Data controller-to-data controller transfers and data controller-to-data processor transfers. The contract clauses for each scenario offer the same protection for the data, which comes down to the parties involved agreeing to the mandatory data protection principals as well as the purpose for the specific data transfer. While this doesn't necessarily offer additional protection for the data, it does explicitly make the parties liable for any violations, in which case the data subjects are entitled to damages.

An agreement containing the standard contractual clauses is an option for properly handling data transfer.

If the data were subject to onward transfers — say from an organization to a law firm and then from that law firm to a litigation technology vendor — the contract clauses must follow the data with all parties agreeing to the terms, with no modifications. While this wouldn't be an issue for litigation matters where transfers may only take place a few times a year, larger matters could require a lot of contracts to cover multiple transfers over time.

WHAT'S NEXT?

The European Commission recently announced that the Privacy Shield, the new EU-U.S. privacy/data transfer pact intended to replace Safe Harbor, would be completed in the second half of February 2016. It considered the recent passage of the Judicial Redress Act of 2015 in the United States, which conditionally extends jurisdiction in U.S. courts to EU citizens for data breach complaints against U.S. authorities, to be "key".[10] Up next, the Commission must pass the Privacy Shield in the form of a decision. It will rely on a group of national data protection authorities known as Working Party 29 (WP29). The group is expected to determine if the framework can pass if tested by the CJEU and will issue its opinion by the end of March 2016.

The EU's Commissioner for Justice, Věra Jourová, was quoted as saying:

> *"The new EU-US Privacy Shield will protect the fundamental rights of Europeans when their personal data is transferred to U.S. companies. 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. Also for the first time, EU citizens will benefit from redress mechanisms in this area. In the context of the negotiations for this agreement, the US has assured that it does not conduct mass or indiscriminate surveillance of Europeans. We have established an annual joint review in order to closely monitor the implementation of these commitments."*[11]

After a two-year transition period, the GDPR will replace the Directive and go into effect in 2018.

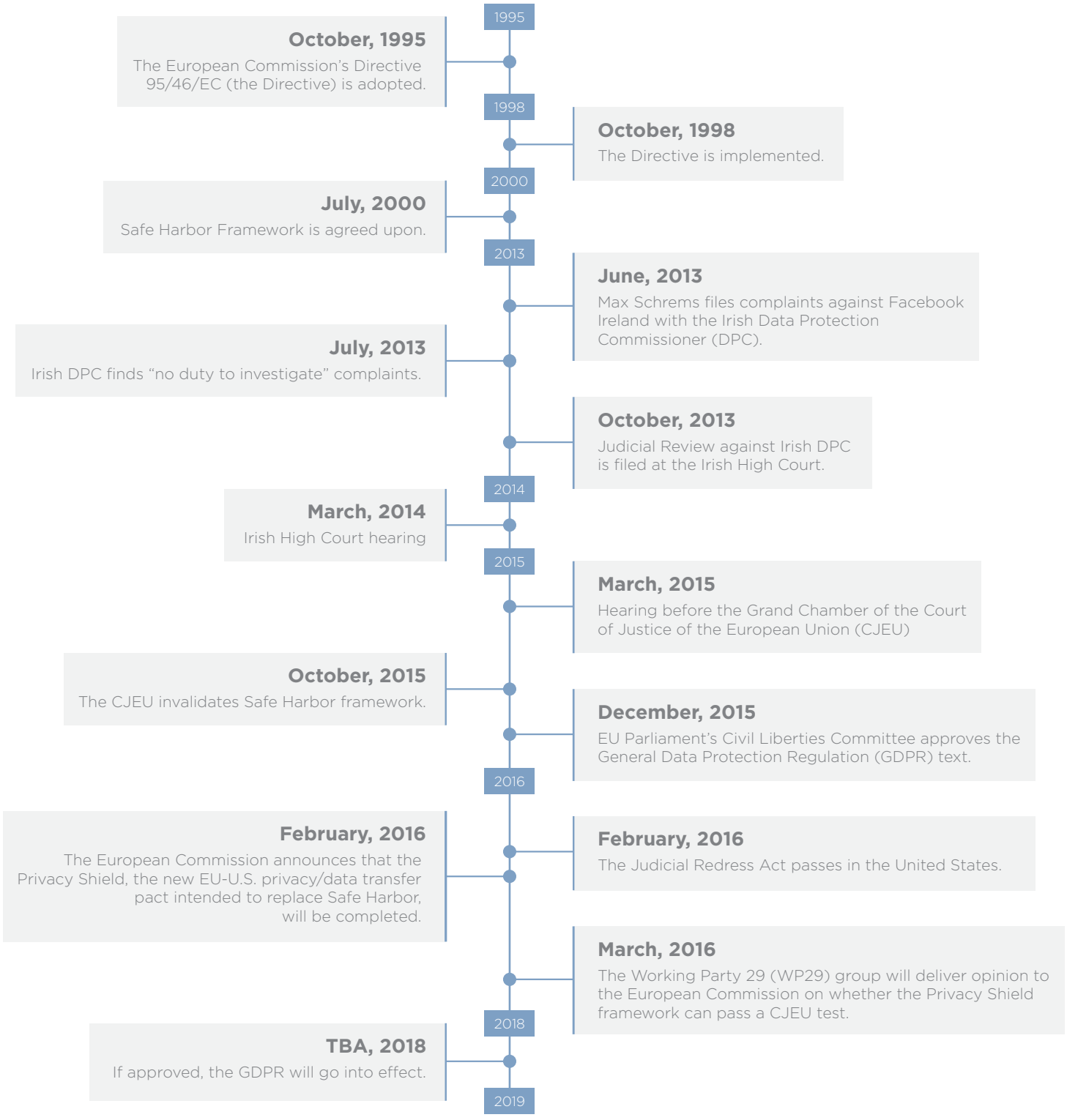
Also on the horizon: Europe's General Data Protection Regulation (GDPR). In December 2015, the EU Parliament's Civil Liberties Committee approved its text. The EU Parliament is expected to officially approve the GDPR by the end of February 2016.[12] After a two-year transition period, it will replace the Directive and go into effect in 2018.[13] The GDPR differs from the 20-year-old Directive in a number of ways, including territorial scope, increased fines for violations, greater control for data subjects, data protection officers and data breach notification.[14]

CONCLUSION

Despite the still-active fronts in the EU and United States to address commercial, legal and privacy needs, an organization can put itself in the best possible position by adhering to the original tenets of the Directive for data protection, asking the right questions, thoroughly documenting processes and closely following the agreed-upon protocols between the parties.

In the event that the new framework does not pass the CJEU's test, it's essential to be proactive and have a data protection plan inplace. In other words, don't let the data protection authorities point it out first.

A BRIEF HISTORY OF DATA PRIVACY AND TRANSFER BETWEEN THE EU AND US



REFERENCES

[1] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[2] Peter Sayeri, *Split Between EU Privacy Watchdogs on Safe Harbor Worries Business Lobby, IDG News Service,* (Oct. 28, 2105), *available at* http://www.cio.com/article/2998636/split-between-eu-privacy-watchdogs-on-safe-harbor-worries-business-lobby.html.

[3] Sebastian Bohme & Christoph Ritzer, *Hamburg DPA Leader Addresses EU-US Privacy Shield*, Norton Rose Fulbright, (Feb. 12, 2016), *available at* http://www.dataprotectionreport.com/2016/02/2831/.

[4] Julia Fioretti, *French Data Privacy Regulator Cracks Down on Facebook, Reuters,* (Feb. 8, 2016), *available at* http://www.reuters.com/article/us-facebook-france-privacy-idUSKCN0VH1U1.

[5] https://www.congress.gov/bill/114th-congress/house-bill/1428.

[6] http://europa.eu/rapid/press-release_IP-16-216_en.htm.

[7] *Id.*

[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

[9] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

[10] Lisa Brownlee, *EC Announces Privacy Shield Timeframe, Conditions, Forbes,* (Feb.8, 2016), *available at* http://www.forbes.com/sites/lisabrownlee/2016/02/08/ec-announces-privacy-shield-timeframe-conditions/2/#57f6ceb34974.

[11] *Supra* note 4.

[12] Raffaele Zallone, *The General Data Protection Regulation: from Promises to Reality, Media Laws,* (Jan. 22, 2016), available at http://www.medialaws.eu/the-general-data-protection-regulation-from-promises-to-reality/.

[13] Courtney Bowman, *GDPR Text Approved, Proskauer Privacy Law Blog, (Dec. 17, 2015), available at* http://privacylaw.proskauer.com/2015/12/articles/european-union/gdpr-text-approved/.

[14] *Id.*