From Safe Harbour to European Data Protection Reform

Tihomir Katulić, Ph.D., Goran Vojković, Ph.D.

University of Zagreb,
Trg maršala Tita 14, Zagreb, Croatia
E-mail: tihomir.katulic@pravo.hr, goran.vojkovic@fpz.hr

Abstract – European personal data protection laws have set the electronic communication privacy standards for more than two decades. Among these standards, the Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament (The Safe Harbour Decision) stood out as a cornerstone of transatlantic data protection regime. The Court of Justice of the EU decision in Maximillian Schrems vs. Data Protection Commissioner in late 2015 has declared the decision invalid. In the light of the long standing legislative reform of the European Data Protection legal framework and the revelations of widely spread unauthorized electronic surveillance, data collection, interception and access by intelligence services and authorities of several countries, there is an urgent need for improved data protection rules, especially regarding collection and export data via cloud services established and hosted outside EU. The purpose of this article is to analyse publicly available reform proposals concerning in the light of the recent ECJ Safe Harbour decision, as well as the developments regarding the future EU-US Privacy Shield proposal.

I. Introduction

In October 2015, the European Court of Justice ruled that the long standing „Safe Harbour“ agreement concerning the transfer of European citizens personal data into the United Stated was no longer valid. The Court, among other concerns, raised the question of adequate protection of European citizens rights following numerous cases of state sanctioned surveillance of electronic communications perpetrated both in the US and among the EU Member States.

Invalidation of the Safe Harbour agreement is a last in the series of developments concerning the development of the European legal framework of personal data protection. Following the landmark Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) in 1995, the Union established what is probably the world's most comprehensive system of personal data protection.

With the exception of Argentina and several other states outside the EU, the level of protection envisaged by the EU framework has not been universally adopted. In this regard, the failure of the US to upgrade its privacy and personal data protection regulation to a more comprehensive system has presented a serious obstacle to future development of services based on collection and use of personal data.

While the new personal data protection agreement between the EU and the US is currently in the works, the strict implementation of EU personal data protection standards may impact the ability of US companies to collect, analyze and store personal data of European citizens.

The aim of this article is to analyze the current legislation reform proposals concerning the EU personal data protection framework with regard to collection, storage and use of personal data by entities based in countries whose legal standards of personal data protection differ from those established by the EU. We will also try to suggest solutions for facilitating a more balanced approach to protection of personal data from the perspective of European citizens having in mind the importance of cloud and personal data based services for the emerging information society economy.

II. Protection of Personal Data as a Fundamental Right in the EU

While it can be argued that most of the now recognized fundamental rights of the European citizens were codified even earlier, the Charter of Fundamental Rights of the EU proclaimed by the European Parliament in 2000 was a first EU document that expressively designates Protection of personal data as a fundamental rights. [1]

The protection is layed out in the provisions of Article 8 of the EU Charter titled "Protection of personal data":

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for the specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access to data which has been collected concerning him or her, and the right to have it recitified.*
3. *Compliance with these rules shall be subject ot control by an independent authority.*

The provisions of the Article 8 effectively create protection of personal data as a fundamental right enjoyed by everyone [1], further enforced by the 2009 Treaty of Lisbon. [2]

III. Safe Harbour Privacy Scheme

After the Data Protection Directive went into effect in 1998, the pan-european data protection standards prohibited the transfer of personal data to countries that do not meet the EU standards of personal data protection.

Following a decision by the European Commission in 2000 that the US personal data protection principles comply with the standards adopted in the EU Data Protection Directive, the US Department of Commerce developed a framework of cooperation with the EU concerning the collection, storing, analysis and use of European citizens personal data under certain conditions.

These conditions were known as Safe Harbour principles: The principle of (giving) notice – the persons whose data was collected had to be informed that their data was being collected and how it was used. Persons subjected to data collection were to be provided with information how to contact the collecting organization with inquiries and complaints. The principle of choice – individuals were required to be allowed the option to opt out of the collection of their personal data and its forwarding to third parties. Principle of Onward Transfer stipulated that data transfers to third parties could only occur when those other parties observed adequate data protection principles. The principle of Security required that reasonable efforts should be undertaken to prevent loss of collected information. The principle of Data Integrity required that collected data had to be relevant and reliable for the purpose it was collected for. The principle of access stipulated that individuals had to be able to access information held about them and correct or delete it if it was inaccurate. Finally, the principle of enforcement required an effective means of enforcing the Safe Harbour principles.

As mentioned above, the purpose of the Safe Harbour scheme was to facilitate export of European personal data to the US in order to be stored, analyzed and used by the emerging information society services (often referred to as Big Data) such as social networks, digital content delivery services etc. European Data Protection Directive mandated Member States implement legal framework preventing export of personal data outside the EU unless an adequate level of protection is guaranteed. [3] In order to facilitate export of personal data to the US, the US companies were allowed to enter the certification program and be certified to adhere to Safe Harbour principles. This was available solely to the US companies and other organizations as regulated by the US Federal Trade Commission and the Department of Transportation and the certification process was not regulated by the Government of the United States. Instead, it was implemented as a self-regulating process through private sector entities with nominal oversight by the FTC and the US Department of Commerce.

The informal, self-certification process was subject to a substantial amount of criticism over the duration of the Safe Harbour scheme. We find these criticisms fully justified. The US Department of Commerce had originally published the set of rules a company or other organization had to follow in order to qualify for the Safe Harbour scheme. However, the self-certification model involved required that participants fill out questionnaires and confirm adherence to Safe Harbour rules. Those who did were entered into the Safe Harbour list without further auditing or supervision. This procedure was both practically unsafe and legally questionable.

IV. CRITICISM OF THE SAFE HARBOUR SCHEME

During the course of the scheme, there have been three external evaluations regarding the compliance of companies and organizations participating in collecting and transferring European citizens data to be analyzed and stored in the United States.

In February 2002, the European Commission published a working paper fulfilling the obligation set in the EU Parliament Decision in July 2000 [4]. The Commission was required to ensure that the operation of the Safe Harbour was closely monitored and to make periodic reports. The report analyzed data from the US Department of Commerce web site, from US public authorities and private sector organizations involved in dispute resolution and enforcing Safe Harbour provisions and from the EU Member States data protection authorities. The Commission concluded that while the required elements of the Safe Harbour agreement are in place and individuals are able to lodge complaints if they believe their rights were being denied, a substantial number of organizations that have self-certified adherence to the Safe Harbour agreement have not established a degree of transparency regarding the fulfilment of their obligations and very few individuals have exercised their right to complain. Furthermore while a wide array of sanctions to enforce Safe Harbour rules under dispute resolution mechanisms were envisaged in the original agreement, not all dispute resolution mechanisms have indicated intention to enforce Safe Harbour rules or have set up in place practices applicable to themselves.

In October 2004, the European Commission published the follow-up working paper [5]. The Commission established that by 2003, there were over 400 US companies that self-certified to the Safe Harbour standards. While the Commission was pleased to see that the provisions of the Safe Harbour agreement were embraced by a large number of US companies, the Commission was concerned about the number of self-certified organizations that have not published a privacy policy or that have adopted a policy non-compliant with the Principles leaving FTC without jurisdiction to enforce the principles of the Safe Harbour agreement. Commission reiterated its previous finding that established alternative recourse mechanisms (dispute resolution mechanisms) still failed to comply with applicable Safe Harbour requirements.

Finally, in 2008 European Commission published a report prepared by an Australian consulting company Galexia. [6] The Galexia report was the most critical to date, revealing of the actual state of protection of European citizens personal data when collected and used by US companies, especially when obtained through new information society services. [7]

In essence, what was considered by many in the EU as a means of providing effective, wide spread protection of EU citizens personal data was in fact a very limited scheme with severe limitations.

The peak number of voluntary participants was less than 3000. [8] Many popular services used by European citizens, such as Instagram, Pinterest, Wikipedia etc., have simply avoided complying with Safe Harbour principles and officially joining the scheme. Additionally, Safe Harbour was originally not applicable to services such as

airlines, banks, credit card companies and telecommunication service providers. [8]

Additional points covered by the Galexia report include transient nature of Safe Harbour protection, false claims of Safe Harbour membership, failure of organizations to provide information to consumers regarding dispute resolution mechanisms, inaccessibility of selected dispute resolution providers to ordinary citizens and the failure of dispute resolution mechanisms to take into account specific Safe Harbour rules etc.

Foremost of them, as stated by the report was the finding that membership status of the organisations in Safe Harbour scheme was not permanent. The report states more than 1000 organisations have left the scheme, and additional number left and subsequently returned. The report stated that there was no accurate list or archive of historic membership and former entries have been known to simply dissapear. [8 p.4]

The report also mentioned a worrying number of false claims in relation to Safe Harbor membership with well over 400 organizations making false claims regarding adherence to Safe Harbour rules in 2013. [8 p.4]

The report states that many of the selected dispute resolution providers are inaccessible to ordinary consumers, jeopardizing one of the most important compliance requirements in Safe Harbour scheme which requires organisations to provide information to consumers regarding dispute resolution. Report finds that key services such as those offered by the American Arbitration Association or the Judicial Arbitration Meditation service are too expensive for ordinary consumers. [8 p.5].

In general, European economy is based on efforts of small and medium enterprizes: “Small and medium-sized enterprises (SMEs) are often referred to as the backbone of the European economy, providing a potential source for jobs and economic growth.” [9] Transition to information society economy has allowed massive outsourcing of previously in house activities, fostering development of micro enterprises (up to ten employees). Lean and flexible by nature these enterprises usually cannot afford information technology specialists. Large organisations (big multinational companies, financial sector companies such as banks and insurance companies etc.) develop their information systems according to current information security standards (ISO 27000 family of standards, PCI DSS etc.) and usually have ample regulatory consulting services.

SMEs, on the other hand, are almost always left to themselves to try to navigate increasingly complex regulatory demands. It is therefore not feasible to expect SMEs to self-regulate - they might be able to satisfy such regulatory demands but in the case they are not, there is no reliable way to ensure their compliance.

V. Personal Data Protection in Europe after Schrems v. PDC

Earlier this year, following a petition by Maximillian Schrems, an Austrian citizen and a user of the popular social networking service Facebook, the Court of Justice has declared that the existing Safe Harbour scheme based on the Commission Decision 2000/520/EC was invalid. Mr. Schrems filed a complaint with the Irish Data Protection Commissioner questioning the efficacy of the legal and practical protection of personal data collected by Facebook and stored and analyzed in the United States, especially against surveillance by the public authorities of the United States. The Irish Data Protection Commissioner rejected the complaint on the ground of the European Commission Decision that established the Safe Harbour scheme between EU and the US. The Commissioner reasoned that under that scheme the US ensured an adequate level of protection for the transferred personal data. [10]

The Court judgement held that the existence of a Commission decision finding that a third country ensures an adequate protection of the transferred personal data cannot eliminate or reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the EU and the Data Protection Directive. The Court stated that even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine whether the transfer of a person’s data to a third country complies with the requirements laid down by the Directive, although it is ultimately the Court's task to decide whether the Commission decision is valid. [112]

The Court further observed that the scheme is applicable solely to the United States undertakings which adhere to it, and that United States public authorities were not themselves subject to it. Since the US national security, public interest and law enforcement have precedence over the safe harbour scheme the Court explained that it was only logical to recognize tha United States undertakings were bound to disregard the protective rules laid down by that scheme where they conflict with such requirements. From the European perspective, this allows United States to interfere with the fundamental rights of European citizens. [10, p.2] The Court observed that any legal framework permitting the public authorities to access on a generalised basis the content of electronic communication to be compromising the essence of the fundamental right to respect for private life [10.p3].

The Court also observed that lack of possibility for individuals to pursue adequate legal remedies compromised the fundamental right to effective juridical protection, and also that denying national supervisory authorities powers to examine the framework of personal data protection was not within Commission competence. (10.p.3].

The outcome of the Court decision was that the Irish supervisory authority was required to examine Mr. Schrem's complaint and to decide whether the transfer of personal data of Facebook's European users to the US should be suspended on the grounds that the US legal framework does not provide an adequate level of personal data protection.

Following the decision by the European Court of Justice abolishing the Safe Harbour scheme the response by the European Commission and the specialized information security agency, ENISA (European Network Information Security Agency) has been lacklustre.

The modern internet is huge - some sources say there are: "over 284 million registered domains… on over 108 million hosts provided… by 5 million computers serving… over 876 million websites.” However, only a tenth of one

percent or less than 1 million account for over half of all web traffic. [11] The most popular Internet services, social networks like Facebook, LinkedIn, Instagram, Google and Youtube, and many other leading services are hosted by companies founded and headquatered in the US. The ruling of the European Court of Justice will have very limited effect on the business practices of companies largely outside of European jurisdiction and US companies will continue to collect and store data on European citizens.

We can observe this even locally. Croatian membership in LinkedIn numbers over 400,000 users, and well over a million and a half Croatian citizens use Facebook. Instagram has almost two hundred thousand users in Croatia [12].

VI. TOWARDS THE NEW SAFE HARBOUR AGREEMENT

In April 2016, the EU Parliament has adopted new data protection rules which now focus on giving the citizens a recourse to take back control of their personal data. The measures adopted also set minimum standards on use of data for policing and judicial purposes, affirming consumer rights and competition in the nascent European digital single market.

Among the new regulations, a few provisions immediately stand out. The new rules enshrine the right to be forgotten, a notion of clear and affirmative consent required by the person concerned as a prerequisite to the processing of private data, a right to transfer persona data to another service provider, the right to know when personal data has been hacked, a requirement ensuring that privacy policies are explained in clear and understandable language etc.

On the enforcement side, the Parliament has adopted measures allowing fines up to 4% of infringers total worldwide annual turnover. Historically, especially in competition cases against US technology companies such as Intel or Microsoft, fines limited to two percent amounted to hundreds of millions of euros, or even 1.06 billion euros (Intel). With this new upper limit, the fines in a potential case against Google could reach up to 6 billion euros.

The new data protection package also includes measures on data transfers for policing and judicial purposes, applying to data transfers across members states and setting minimum standards for policing purposes within each member state.[13]

. Earlier this year, the European Commission and the United States have agreed on a new framework for transatlantic data flows: the EU-US Privacy Shield.

The new arrangement will include the following elements:

First, strong obligations on 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.

Second, clear safeguards and transparency obligations on U.S. government access: For the first time, the US 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 US under the new arrangement.

Thirdly, 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 Trade Commission. In addition, Alternative Dispute resolution will be free of charge. [14]

These provisions represent a significant step ahead with regard to the old Safe Harbour self-evaluation model. Further research, especially of the practical side of the implemented model is required. The EU needs to adopt a model of regular independent audit concerning the implementation of the new regulation and the new data transfer scheme.

VII. CONCLUSION

The existing European legal framework regarding personal data protection is based on two main pillars, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108) Council of Europe, and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive provisions have been widely adopted and implemented as were the principles of data protection from the CoE Convention.

Faced with recent challenges, such as Snowden revelations and other instances of illegal and unsanctioned access and interception of personal data and communication it is clear that existing framework is showing its age.

While new personal data legislation, this time in form of a binding regulation is scheduled to be introduced very soon, the practice of personal data protection is something that needs to be addressed on political and economic levels as well as legislative. The measures adopted by the European Parliament and the future EU-US Privacy Shield might very well improve the state of personal data protection for the citizens of the European Union. However, in order for these improvements to truly come about a vigilant survey of the application of the new regulatory model is required, especially in the light of previous efforts and practical results.

REFERENCES

[1] Fuster, Gloria Gonzalez: The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law,

Governance and Technology Series 16, Springer International Publishing Switzerland, 2014

[2] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, [2007] OJ C306/1.

[3] Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such dataEuropean Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)

[4] The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC(2002) 196., available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/sec-2002-196_en.pdf

[5] The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC (2004) 1323, available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/sec-2004-1323_en.pdf

[6] "The US Safe Harbour – Fact or Fiction", Galexia Pty Ltd., 2008., http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (22.2.2016)

[7] EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance, http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf (22.2.2016)

[8] Connoly, Chris: EU/US Safe Harbor – Effectiveness of the Framework in Relation to National Security Surveillance, Galexia, Speaking / background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on "Electronic mass surveillance of EU citizens", Strasbourg, October 7 2013, available at: http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf (22.2.2016)

[9] http://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme?p_p_id=NavTreeportletprod_WAR_NavTreeportletprod_INSTANCE_vxlB58HY09rg&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=4 (22.2.2016)

[10] European Court of Justice, ECJ Case C-362/14 Maximillian Schrems v Data Protection Commisioner http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (22.2.2016)

[11] http://tekeye.biz/2014/how-many-websites-are-there (22.2.2016)

[12] http://www.netokracija.com/broj-korisnika-instagrama-u-hrvatskoj-108541 (22.2.2016)

[13] Personal data protection: processing and free movement of data (General Data Protection Regulation), http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en, (14.4.2016)

[14] EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield http://europa.eu/rapid/press-release_IP-16-216_en.htm (29.4.2016.)