GIZEM GÜLTEKIN VÁRKONYI*

International Personal Data Transmission: European Union Approach

Introduction

The technology in the 70's and on the 21st century definitely is not same. Software and hardware combination is just like one of our organ anymore. The engine of the such developments work with big amount of data. If a user accept to throw his or her data into the unknown space, then it is possible to benefit from services that makes life way much easier than manual processes; this is where we are. However, it is one of the fundamental right to get to know the unknown space and control it as the owner of the space is already the owner of the content of it.

Development of software and hardware technology mainly speeded up in the 90's especially when Vannever Bush invented the internet. Since then, perception of privacy was not something borderless. This movement was mainly because people started gaining information and sharing information on the virtual space. By sharing information of themselves, they expressively created their virtual identity. This identity consists of many private data regardless of its share with will or without. Privacy used to refer to the physical privacy referring to family life and protection of someone's physical space. Virtual boom carried the privacy perception to the other concept either

Protection of personal data as a single fundamental right was accepted firstly in many of the European countries' legislation. The basement of such development is that because the European people learnt well about the history. They already knew that their own personal data sometimes can be used against themselves especially if it will be serving for political or ideological goals. The starting point may be accepted when an individual asked to get to know about how and why authorities of German Land, Hesse, keeps and processing his personal data.[1] Similar to that, in Sweden, Portugal, Spain and then in many countries realize the fact that personal data protection is a human right and it should be indicated in the legislation. Meanwhile, the US citizens were also demanding to get know about how the US banks use their personal data that was given for the mortgage processes. By 80's, many

* PhD Student, Doctoral School of Law and Political Sciences, University of Szeged.

[1] KÜZECI, Elif: *Personal Data Protection.* Unpublished doctoral thesis, Ankara University Institution of Social Sciences, Ankara, 2010. 117-119.

country was in the point to announce their legal modifications on understanding of privacy. Furthermore, the realization of personal data protection as a fundamental right in an international sphere was expressed by the international organizations such as the United Nations, Organization for Economic Co-operation and Development, Council of Europe and European Union.

Privacy was expressed as a fundamental right in various international legal instruments, firstly in the United Nations, 1948 Universal Declaration of Human Rights, then Council of Europe 1950 the European Convention on Human Rights. However, when the electronic and digital systems, or devices like computers, smart phones, or online tools such as online booking systems, are developed and integrated in the individual's life, traditional privacy protection measures start not to meet the current needs. On one hand, if people do not use such systems, they may have to pay more for some certain services, for example, buying plane tickets online is always cheaper than buying it from an agency or over the phone. On the other hand, if there is not enough legal protection, the blessings of technology may turn against the individuals and cause them more harm than a good. Within these developments, privacy could be positioned in different contexts such as information privacy, spiritual (decisional privacy) or physical privacy (e.g. home, family).[2]

Personal data is once collected, it can be used as a "dataveillance" tool by the governments to give an opportunity to monitor ordinary people.[3] Furthermore, it is known that governments not only watching their own citizens; but also other governments and their citizens. When the Former National Security Agency, Edward Snowden disclosed the fact that the Agency watches many countries' activities, it received many criticism.[4] The tension became that much high, it even affected the US and the EU relationships. One of the reason behind cancellation of the Safe Harbor was the EU's opinion on a possibility of misusage of large personal data by the US. For this reason, wherever data transmission is foreseen, the transmission rules and further implications should be well discussed and should have well structured legal basement.

This article will show some of the practical problems related to cross border data transmission issues and the solutions. The EU and the US personal data transmission relationship will be chosen on the ground of security and commercial aspect. In frame of this, the EU-US Passenger Name Records agreement and Privacy Shield agreement will be presented. These agreements are important to enhance the EU's personal data relationship with third countries if they comply with the basic rules referred within these agreements.

Transmission of Personal Data in the International Legal Documents

Transmission or transfer of the personal data means that the data leaves the country of the origin and become a property of the recipient country. During the transmission, the personal data may pass thorough different countries, however, where the data processing

---

[2] SAVOIU, Alina – BASARABESCU C. Capatina: The Right to Privacy. *Annals of the Constantin Brancusi University of Targu Jiu Juridical Sciences Series* 1 (2013) 92.

[3] EIJKMAN, Quirine: *Counter-Terrorism, Technology and Transparency: Reconsidering State Accountability.* The International Centre for Counter-Terrorism, The Hague, 2012. 3.

[4] FARELL, Henry – NEWMAN, Abraham: The transatlantic data war: Europe fights back against the NSA. *Foreign Affairs VO* 95 (2016) http://search.ebscohost.com/login.aspx?direct=true&db=edsgao&AN=edsgcl.439135741&lang=tr&site=eds-live&authtype=ip,uid (2016. 12. 27.); GILES, Courtney: Balancing the Breach: Data Privacy Laws in the Wake of the NSA Revelations. *Houston Journal of International Law* 37 (2015) 552. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=102839256&site=ehost-live (2017. 03. 22.)

activity starts, there should be named as a recipient country. Since the mass technology usage have combined with systems where the data is stored in a physical storage that possible may be outside of a certain country, transmission action already have been going on. Such combination have boosted with the invention of Vannever Bush, the internet. From his invention to now on, we are at the position to share information on a nearly light speed.

These issues must be foreseen by the international organizations in the beginning of development of personal data protection legislation. Nearly all international personal data protection document mentions about the personal data transmission outside of jurisdictions. First step was taken by the Organization for Economic Co-operation and development in 1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data aims to be bridge between the countries to create basic framework for personal data transmission for commercial and economic development while respecting to human rights. The guideline targets to give minimum standards for both national and the international level of personal data processing. According to the Guideline, the basic principles are listed as:

– The data should be collected in frame of law and data subject's consent (collection limitation)

– The data should be used only for its purpose, and should be accurate, complete and up to dat (data quality)

– The purpose of the collection should be specified and should not exceed it (purpose specification)

– The data should not be disclosed for other other purposes (Use limitation principle)

– Recipients should take necessary steps to protect the data (Security safeguard principle)

– There should be available information about the data's lifetime (Openness principle)

– Data subjects should be able to get confirmation from a data controller if the data controller holds any data related to them; ask for change, erasure, rectification or amendment if the data is used outside of the scope (Individual participation principle)

– Data controller should follow the Accountability principle to prove that it complies with the principle.

Basement of the Guideline is not to restrict free flow of data for economic development but there exception rules that can interrupt the personal data transmission. As it is a guideline that cannot bind the national security issues, it gives exceptions for the principles on the ground of national security, national sovereignty and public orders.

The document was the first of its kind dealing with transmission of personal data outside of jurisdiction and evaluated as it received the widest acceptation even though there are countries with different perception on data privacy such as Germany, the United Kingdom, Canada, United States, Japan, and Korea[5] The principles can be found as a basement of the other international legal documents as well, so we will not repeat these principles. Even though revision of the Guideline to meet with the dynamic privacy needs was a bit late, the document now covers most of the privacy concerns in general. Revised in 2013, the Guideline now focuses on a practical implementation of the principles and

[5] DE HERT, Paul – PAPAKONSTANTINOU, Vagelis: Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? *Journal of Law and Policy for the Information Society* Vol. 2., 9 (2013) 277.

more intensive privacy cooperation among the member states through strategies and programs.

As we have indicated before, European countries were the first ones that took steps towards developing the privacy and personal data protection legislation. Only a year after, in 1981, Council of Europe opened for a signature of Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Importance of the Convention is that it is the first legal document bringing the "adequate level" rule for data transmissions[6]. Amendment to the Convention 108 in 1999 opened the document for non-members as well. In 2004, additional protocol applied to the Convention including regulate on the "*Transborder flow of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention*". The adequacy rule was stressed out here in frame data transmission to the non-signatory countries or organizations if they ensure the adequate level of protection for the demanded data. The adequacy means that the non-signatory party should ensure the Convention safeguards in the national law or if there is a specific interest to the such data for public interest and specific interest to the data subject.[7]

It can be assumed that the adequate level of protection expression was heard more with the EU legislation. As a biggest trade partner of each other,[8] EU and the US run many businesses and collaborations. EU's personal data protection legal framework is mostly based on the Convention 108. However, personal data transmission rules shaped and developed more in the EU legislation than any other document. This may be explained as the EU already knew well the fact that there is a distinction between the EU and US perception on privacy. In 1995, EU's "*Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*", known as European Data Protection Directive (Directive) signed. In 2007, personal data protection right exclusively expressed on the Charter of Fundamental Right so the EU institutions are also abided by the Directive rules.

The Directive's adequate level expression is important because it is the first document which conceptualize what does the adequacy means in frame of transmission of personal data to the third countries. Adequacy rule is a rule to decide for the Member States whether they would like to permit or prohibit the transmission. Evaluation of the data requester body in frame adequacy is mostly left to the national decision-makers. During the decision making, third country's national law and international commitments are being evaluated but specifically as the Article 25 specifies:

– the nature of the data,

– the purpose and the duration of the processing,

– the country of origin and country of final destination,

– the rules of law, both general and sectoral, in force in the third country in question and

[6] Id. 275.

[7] ETS 181, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows Strasbourg, 8. XI. 2001.

[8] "Compared with the other major world economies, the United States and the EU recorded among the highest values for trade in goods 2013 data" Eurostat. http://ec.europa.eu/eurostat/statistics-explained/index.php/USA-EU_-_international_trade_and_investment_statistics (2017. 03. 19.)

– the professional rules and security measures which are complied with in that country, should be evaluated to decide whether a third country is falling under privacy safety country.

Although the third country does not fall into the privacy safety countries list, and if the transmission is still necessary, then the transfer may occur if, data subject's "unambiguous" consent exists; needed for performance of a contract clauses; needed for conclusion of a contract between the data subject and the third party organization; needed to protect public interest; to protect the interests of the data subjects and; if the third country ensures additional safeguards for the particular transfer or transfers.

It is the Commission that the Member States comply with the decisions of and inform about the authorizations of a third country transmission. Also, the Commission can propose any measure to the Council upon the breaches to the Directive. The Commission acts in parallel with the Council recommendations or can make its own decisions.

However, Directive 95 of the EU soon will replace with the GDPR which is not as strict as the Directive from the data transmission point of view. Within the GDPR, it is possible to transmit personal data outside of the EU where there is no adequate level of protection. It is possible if the third country ensures minimum level of safeguards such as the purpose limitation or if the transmission is necessary for public interest such as security. Previously, the 95 Directive strictly prohibited the personal data transmission to the third countries. The GDPR focuses more on the data subjects' rights rather than restricting data transmission. By this way, the third countries always will have possibility to gather information for on-case situations. We believe that the new GDPR will cause some modifications on the current data collaboration agreements between the EU and the third countries.

We tried to draw the whole adventure of the data protection in Europe. We exclude the new General Data Protection Regulation of the EU which will enter into force in 2018 May, because we would like to summarize practical problems and the solutions regarding to cross-border data transmission, especially to the countries where there is not enough legal ground for privacy protection. Here, we focus on the EU-US personal data collaboration history in order to reflect a practical sample for the third countries offering no adequate level of privacy protection but, has to collaborate with the EU for security and/or commercial reasons. There are two well known EU-US collaboration example falling into these topics: EU-US PNR Agreement and the Privacy Shield.

Personal Data Transmission for National Security

Rising amount of the terrorist activities in the US and especially after the 9/11, the United States government(s) have been still taking security measures today even stronger and stricter ones. The Personal Name Records program is one of the security program supporting law enforcement bodies to control the migration traffic. With the help PNR profiling, law enforcement agencies can once again evaluate the passengers on the way to the US, whether they might be dangerous for the country or it is safe to permit their entrance. Wishing this program, the US authorities oblige all the air companies to transfer PNR data before the flight so they can have one last check on the passengers.

According to the International Civil Aviation Organization (ICAO),[9] PNR means in the air transport industry is the generic name given to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger. Passengers either may type these data themselves or may give the data to the travel agents to complete their reservation process on the electronic reservation systems. All information stored in the (databases) reservation systems with the relevant information as well as some of the updated ones. The full list of the data required for creating a PNR data are 22 of them in total according to the ICAO documents. This digit number is stored in the computer systems and these systems can transfer it to the other same systems.

PNR data is different than the visa, passport, biometric and other ordinary data that is given to the law enforcement bodies by the migrants. These data are both case-based and general personal data. It is case-based because it gives instant information about a certain flight such as seat number, meal choice, baggage information etc. It also falls within general personal data category because it gives basic information about the passenger such as name, address as well as financial information. Although the reason behind creation of the PNR was to give passengers better and on-time services, it is now being used as a tool for national security.

Almost all of the international legal documents and guidelines addressing personal data transmission include some exception rules for personal data transmission for national security. However, where there is no such strong or no legal framework for privacy protection, there will be no control over wrong implementations such as surveillance and misusage. Basic principles actually save people from being a suspect of crimes or terrorism. They save people from being watched everyday on wherever they are. The legal insurance save the society from racism, discrimination and xenophobia.

Still, the importance of the PNR data is not restricted with its content that is helping to identify the people (terrorist or not), but its power to help to the law authorities to make risk assessments, make decisions and keep the experience for the further decision making issues. All these steps can be taken only if the data is accurate and updated enough to make correct identification, that is why, PNR data is giving a well structured ground especially from the accurate and updated point of view. Earned-experiences also can be shared with the other countries so it can help to create safer globe.

Increasing number of terrorist attacks as well as the brutality and its global effects put every country into a situation where they must collaborate more to defeat terrorism. Some of the members of the European Union as well as some of the candidate countries, for example, Turkey, faced with serious terrorist attacks within the last 10 years. The EU is open for any solution in a legitimate basis and respecting to human rights. Hence, the US PNR program somehow perceived as a forced action. On one hand, all air companies as well as the EU based ones obliged to transfer the PNR information which has a legitimate based in the US law but not enough for the EU in such a way that the purpose restriction and further processing activities are not clear. For this reason, air carriers as well as their country of headquarters were at risk of breaching the EU law. On the other hand, there was a big risk to be punished by the US law enforcement agencies, if they do not transfer it. For this reason, EU prepared its legitimate basis for both protecting the companies

[9] ICAO: *Guidelines on Passenger Name Record (PNR) Data*, 2010. https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf (2017. 03. 20.)

financial interest and the EU citizens' fundamental rights, while respecting to the US national security programs. In 2004, EU and the US signed the first PNR agreement.[10] However, only after 2006 European Court of Justice annulled this agreement based on:

– The Commission is not a competent body to conclude such agreement in name of the Community based on Treaty of Functioning the European Community[11] and

– It is not clear in the agreement "the adequate level of protection for the transferred PNR data" which breaches the Directive in such

– The method (pull method)[12] of the data collection is not an appropriate method for data transmission,

– Number of data element to be transferred is more than necessary

– The purpose of the data collection is not clearly defined,

– The data storage period is longer than it should be.[13]

Rising terrorist attacks in Europe taught well the importance of global collaboration to fight against terrorism to the Member States. Although the divergence between the members to allow data transmission to the US, 2004 PNR Agreement revised and interim PNR Agreement signed between the EU and US in 2006. The 2006 interim agreement switched with the 2007 PNR Agreement and could last until 2012 when the agreement renewed. Currently, the EU and the US ongoing the PNR collaboration and it will last until 2019, if the new General Data Protection Regulation of the EU does not affect the agreement entirely. Currently, the EU have PNR agreements with Canada since 2006 and Australia since 2012, and negotiations with Mexico on the way since 2015. Moreover, in April 2016, the EU adopted a Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The Directive basically draws a framework for sharing between and usage of the PNR data by the law enforcement agencies of the Member States for preventing terrorism and organized crime while respecting the air passengers' rights.[14] These developments all mean that the EU takes PNR usage and share as well as personal data for security. It is also clear that the EU will widen its collaboration with third countries for personal data transmission. For this reason, EU is ready for such agreements with third countries in frame of its basic principles. These basic principles are drawn under the EU Global Approach to PNR transfers communication document. It is an important document because it sets out "*general criteria for EU's bilateral agreements with non-EU countries on transfers of PNR data in order to harmonize transmission modalities and provisions on data protection*".[15]

---

[10] 2004 Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security,Bureau of Customs and Border Protection. http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf (2017. 04. 04.)

[11] European Court of Justice, Judgment of the Court of 30 May 2006. European Parliament v Council of the European Union and Commission of the European Communities, Protection of individuals with regard to the processing of personal data -Air transport-Decision 2004/496/EC. http://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=954501 (2017. 04. 02.)

[12] The system permits data transmission as long as the requester pulls the data from it.

[13] Id. 11 (e).

[14] OJ L 119, 4.5.2016. 132-149. http://eur-lex.europa.eu/eli/dir/2016/681/oj (2017. 04. 02.)

[15] COM(2010) 492 final – Not published in the Official Journal.

The Global Approach document was first prepared in 2003 but changing nature of the technology, security and its effects on personal data protection right caused a need for review on it which occurred in 2010. The document sets out some of the Principles that can be cataloged under "General rules and principles"; "Transmission and processing rules"; and Passengers' rights. General rules and principles put the operational rules such as accountability, reciprocity, monitoring and dispute resolution. Transmission and processing rules foresee the technical and practical implementation of the agreement while the data transmission occurs such as method of transfer, limitations, restrictions, frequency, and security. Principle of Automated Individual Decision also involves into this category because this principle forbids the decision-makers to only rely on software or machine based filtering systems while they do decide about a person's risk to the national security. Passengers' rights on their own data is few but enough for now. Right to be informed about their data usage by the law enforcement agencies; accession, rectification and deletion of their data; and redress mechanism for them to apply for in case of misuses are some of their rights under this document. If the new GDPR affects this document for change, we believe that it will change mostly right of the passengers' part. The GDPR give more rights to the data subjects, such as right to be forgotten.

There is another agreement between the US and the EU signed to fight against terrorism especially from a financial point of view. The Terrorist Finance Tracking Program (TFTP) which is a successor of non-born SWIFT[16] agreement was prepared upon the US's demand to track the terrorists' financial network and it was another tool to enhance the national security in the US after the 9/11. SWIFT data basically contains any financial transaction history of the bank account holder as well their identical information such as name, address, national identity number etc.

Right after the 9/11, the US authorities started to use SWIFT network to identify, locate and track down people suspected of terrorism.[17] The data is accurate, classified and shows very specific and useful information such as the sender/receiver information while money transaction. Unless such data was only stored only in the US servers, data was treated as a US property. However, SWIFT providers has started a new messaging architecture from 2009, which includes server possibility also in the EU.[18]

The US would not have access to the EU based server in this case. Moreover, the EU also realized the importance of such data for identifying illegal financial path.[19] For this reason, EU has speeded up framework preparation which has been undergoing since 2007. First SWIFT agreement draft was voted down by the European Parliament, not as a result of a surprising reason: inadequate protection. Reasons of the inadequate protection was more or less same as the PNR agreements discussions: time limit, purpose limitation, data storage period and data retention frequency were some of the known problems. The

[16] SWIFT actually does not refer to anything numerical but it is the organization's name's abbreviation that is "Society for Worldwide Interbank Financial Telecommunication" located in Belgium. The organization's financial services especially secure financial messaging services has made it well-known.

[17] See the explanatory post online: http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20100205BKG68527&language=EN (2017. 04. 08.)

[18] COM(2013) 843 final. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/news/news/docs/20131127_tftp_annex_en.pdf (2017. 04. 08.)

[19] Id. The report summarizes some of the personal data usage cases gained through TFTP agreement to disclose terrorist related activities or connections. EU and Member States used such data to find out activities belonging to different terrorist groups such as PKK, Hamas, Islamist terrorists, Sikh and IJU.

second SWIFT agreement, which is TFTP now, was developed with several functions such as function of the Europe and Eurojust to have an active role to receive/deliver the financial messaging data. Furthermore, not only the institutional engagements but the agreement itself is different from the PNR agreement by nature. The PNR agreement foresees to transfer all the passengers's data regardless of their situation whether they are terrorist or under investigation. SWIFT data can be sent only if the data subject is already known as a "dangerous person" for the national security; identification of the person has already been made by the law enforcement bodies. Another difference between the TFTP and PNR agreement is that data can be transferred only if one of the party request and only if the competent authority permit the transmission Moreover, the data can be only used for prevention, investigation, detection, or prosecution of terrorism or terrorist financing.[20] For these reasons, we exclude this agreement to review more detailed in this work, but it is important to indicate that the TFTP agreement also complies with the adequacy principles drawn in the Global Approach document although it was prepared for the PNR transmission.

All the steps were taken by the EU authorities as well as the Member States to fulfill the huge gap between the technologic development and legal developments while fighting against terrorism. It is clear that protection of personal data legislation cannot catch the speed of technology, so that there is a need to revise it on time. While pulling up the data protection standards to the current needs in one jurisdiction, it is also important to be sure whether these standards are acceptable by the possible partner countries. We think that both the PNR agreement model and the Global Approach document is giving minimum standards for data transmission and collaboration standards for the current needs.

Processing of Personal Data for Commercial Reasons

According to the DLA Piper's research, one of the most data security breaches occurs in the financial sector. Then, it is followed by the Technology, and Health Care and Life Sciences sectors.[21] As the US is a major trade partner of the EU on both good and services,[22] it might be expected that a large personal data flow occurs everyday between these partners. This expectation must be foreseen by the EU authorities in the early 2000s. In order to not to put the businesses in pressure so that would not cause the good relationship to be broken, the EU and the US agreed on Safe Harbor principles.

Even though the Safe Harbor agreement is not valid since 2015, it is important agreement in a way that it is the first and long-last privacy agreement between the EU and the US permitting data transmission for commercial reasons. The basic aim of the Safe Harbor agreement was to ensure data privacy of the EU citizens while they receive certain services from the US companies. The reason why behind the such agreement is that the US sectoral approach to privacy while the EU accounts it under fundamental rights which also

---

[20] L 195/5, Article 3.

[21] DLA Piper, *Global Data Privacy Snapshot 2017: How does your organization compare?* https://www.dlapiper.com/en/uk/insights/publications/2017/01/global-data-privacy-snapshot-2017/ (2017. 04. 01.) It is a complimentary survey which poses a series of questions relating to 12 areas of data privacy, such as privacy policies, the use of data, security measures and individuals' rights. January 2016, and in the year since then, over 250 organizations from 13 different sectors have completed the online survey and 136 organizations are the global companies.

[22] EU and US form the largest trade and investment relationship in the world Eurostat. http://ec.europa.eu/eurostat/statistics-explained/index.php/USA-EU_-_international_trade_and_investment_statistics#EU.E2.80.93US_trade_in_goods (2017. 03. 18.)

affects the legal structure. The EU acquis as well the Member States' constitutions undertake privacy as a fundamental right and make comprehensive legislations with rules, obligation and independent enforcement bodies while the US makes it at the regulation level. The organizations act in the EU land as they do in the US which causes contradiction to the basic understanding of privacy.

Safe Harbor agreement was found invalid by the ECJ in 2015, after 15 years of enforcement, giving as a reason that "the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country"[23] meaning that the adequate level of protection has not ensured by the US authorities. In fact, Safe Harbor does not cover the US public authorities to access EU citizens' personal data. Invalidation of the agreement would not mean the end of commercial cooperation between the EU and the US. In 2016, without a long break, the transatlantic partners concluded another agreement called Privacy Shield which replaced, as well as developed, the Safe Harbor agreement. It brings stronger obligations for the companies while more enhancing the rights of the data subject. It also clarified the institutional mechanism.[24]

Privacy Shield agreement was signed upon and once again to ensure the data "adequacy" rule of the EU. In order to comply with the rule, couple of recommendations were prepared based on practical experiences and legal review. These recommendations focused on strengthening the substantive privacy principles, increasing the transparency of U.S. self-certified companies' privacy policies, better supervision, monitoring and enforcement by the U.S. authorities of compliance with those principles, the availability of affordable dispute resolution mechanisms, and the need to ensure that use of the national security exception provided in Decision 2000/520/EC is limited to an extent that is strictly necessary and proportionate.[25]

Privacy Shield now cover 1916 US based organizations[26] which were self-certified by the US Department of Commerce upon the application of the organization. Certifications are valid only for a year and if the organization does not re-apply for the certification, then it will not benefit from the Privacy Shield Program. The companies that breach the privacy rules of the Program can be dismissed from the Program, as the new approach brought as a rule.

The Program offers number of benefits for the EU citizens whose personal data is being transferred to the US organizations:[27]

Right to be informed, access and correct the data, refers to get know about the personal data's lifecycle by the data subject. Right to know the types of the data, reasons for

[23] Case brought by the Austrian student to the Irish court (because of the country of residence of Facebook headquarter) was related to his personal on Facebook that was shared with the National Security Agency for security or surveillance reasons. Irish Court asked for a preliminary ruling from the ECJ, and case called Maximillian Schrems v Data Protection Commissioner resulted with invalidation of the Safe Harbor Agreement. Court of Justice of the European Union Press Release No 117/15. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (2017. 03. 20). The ECJ court full decision is accessible online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 (2017. 03. 20.)

[24] COM(2016) 117 final.

[25] C/2016/4176 OJ L 207, 1.8.2016. 1–112. http://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj (2017. 03. 21.)

[26] Privacy Shield Program website: https://www.privacyshield.gov/welcome (2017. 04. 07.)

[27] COM(2016) 117 final and 12 July 2016 Press Release entitled European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows.

processing and/or transferring to other organizations, and accession right to own data rules were already mentioned in the Safe Harbor. The new rights with the Privacy Shield program are: Right to withdrawn from the consent and authorization of the US Ombudsman for the complaints of the data subjects. Data subjects also may ask for the reasons for data processing, types of data that is being processing and the other third party accession to the date if there is.

Limitation of the personal data usage out of its purpose, that is the basic principle referred in the all EU legislation related to personal data and personal data transmission. Usage of the data for its directly original purpose of collection and usage which is related to or close enough to its original purpose is allowed.

Time limitation and data minimization, reminds the conditions in the PNR agreements, and refers to keep the data only until it is needed and to collect only necessary amount of it.

Security insurance, refers to technical safeguards against leaking, misuses, disclosure and other risks for the personal data.

Data transmission rule, refers to the data transmission from the first receiver company to the other company if it also complies with Privacy Shield principles.

Remedies and complaints refers to the mechanisms that the data subjects' may apply for if they think that there is a breach of the Program. Safe Harbor also offered such mechanisms but with the Privacy Shield, new mechanisms are added. These mechanisms are the Privacy Shield Panel, Ombudsman, Alternative Dispute Resolution and the Privacy Shield Program certification holder which is the company itself. The US Department of Commerce and the US Federal Trade Commission will be indirect mechanisms because they will act if the cases are referred only by the Ombudsman.

Privacy Shield also brings the two partners closer in such a way that there would be regular joint reviews for monitoring the functioning of the Program. The reviews will be held every year and the partners will work to improve execution of the agreement based on their experiences.

Transatlantic partners could solve two problems at one agreement: the risk of breaching fundamental rights of its citizens and the obstacles standing front of the trade partnership. Privacy Shield is another good example how the EU is cooperating with the third countries and creates win-win situation for the Union. What is eye catching that although EU is in trade relationship many other third countries, privacy agreement only exists with the US. This might be because the US is one of the biggest service provider in financial sector and online services as well as software technology. It is also true that the EU offers data protection right to any person regardless of their nationality or citizenship.[28] However, as long as the EU has been trying to standardize protection measures everywhere in the world for its citizens, there should be more data privacy partnership agreements with the other third countries, for example with China, that can prevent EU from harms towards its privacy sensitivity.

[28] The EU offers its privacy protection to some of the third countries for example China, Turkey and Mexico, through Privacy Policy Statement in trade. The EU informs these trade partners about how trade related data of their citizens and how it is being processed, for what reasons and what might be the remedies for certain circumstances. See the agreements: http://trade.ec.europa.eu/doclib/cfm/doclib_section.cfm?sec=706&langId=EN (2017. 04. 07.)

Conclusion

Protection of personal data has been in a debate since the technologic developments heavily and continuously gather such data for certain purposes. In cases such as misusage or data-leaks, the data protection even become more important from the fundamental point of view. Internet and its borderless nature make the personal data's adventure hard to follow especially if the data subjects would like to get know why, where, until when, and how their data is being processed. Even though there are international standards and guidelines, it is not easy to standardize the protection at the national level.

European Union puts the most effort to balance between the fundamental rights of its citizens and relationship with the third countries. The EU is open for any kind of collaboration with the third countries if there is a legal protection for its citizens. Importance and need for personal data increases for national security and commercial activities which also might need to be transferred outside of jurisdictions. Hence, cases such as rising amount of terror attacks or non-EU based servers to store personal data collected for commercial reasons triggered EU Member States as well as the Institutions.

The EU mostly in relation as well as in conflict with the US understanding of privacy. They are one of the best partner in trade and joint collaboration in fighting against terrorism. This partnership based on a success of the EU consistency on creating global standards for protection of fundamental rights and right to protect personal data. EU-US PNR agreement and Privacy Shield agreement has long but successful story from the protection of rights of the people's personal data. We believe that these collaborative actions on the well-structured agreements will be sample for other countries that are in commercial relationship with the EU and for the countries that need to gain personal data from the EU citizens to enhance its national security programs.

GIZEM GÜLTEKIN VÁRKONYI

International Personal Data Transmission: European Union Approach

(Summary)

Transmission of the personal data outside of the national jurisdiction has always been a debate at the international level. It is because, for instance, online service providers that offer their services based on personal data can be located in different countries or growing security threats make the personal data necessary to be a part of an intelligence that should be shared with other countries for the world peace. On the other hand, different understanding of privacy between the countries may cause breach of personal data protection right. Some of the data transmission conflicts between the United States and the European Union regarding to transmission of the personal data could be solved with bilateral agreements and they became a model for the EU for further collaborations with the third countries.