Centre for Economics and Foreign Policy Studies

EDAM Cyber Policy Paper Series
2016/3

Cross-Border Data Transfers and Data Localization

June 2016

Asst. Prof. H. Akın Ünver
Board Member, EDAM

Faculty Member, International Relations,
Kadir Has University

Grace Kim
Research Assistant, EDAM

EXECUTIVE SUMMARY

In March 24, Turkish Parliament approved the Law on the Protection of Personal Data, which was put into effect by April 7. The much debated law entered into effect with profound problems, most notably in aspects such as the definition of personal data, a broad list of exceptions to the law and the composition of the Personal Data Protection Board as a political body, instead of a technical one. Most recently, the e-money operator PayPal withdrew from Turkey, citing incompatible regulatory requirements, the most important of which was data localization.

This paper offers an introduction to the debate on data transfers and localization, why companies store data and how regulation-versus-localization shape the debate on data transfers. Then, it discusses more technical aspects of how governments regulate data transfers, why they want to localize data and the pitfalls of over-regulation in data management. Finally, we look at the specifics of Turkey's data localization requirements for foreign companies and how the recently passed law on personal data protection falls short of addressing Turkey's data policy needs. We argue that the only way forward for Turkey is to adjust its data protection law into a more democratic, transparent and technocratic code, with a special emphasis on freedoms, rather than surveillance intent.

INTRODUCTION

The history of trade evolves around means and methods that render the transfer of goods and services in the most efficient way possible. During the Silk Road period for example, the development of the idea of a caravan – a mutually supporting group of traders and journeymen – substantially improved the economies of scale in trade and allowed luxury goods to reach parts of the known world that they otherwise never could. Then the invention of sailing and the rise of merchant ships substantially increased the volume of goods being transferred to an even wider geography. A single early-medieval cargo ship for example, could transport three times more goods than a 500-camel caravan across the Silk Road. In response, not only did the scale of trade and size of the economies of the known world expand, but the center of gravity for world trade also changed, leading to the rise of new powers. In the subsequent centuries, inventions of more efficient methods of sailing, of flight, and of steam engines all contributed to globalization, the expansion of trade, and the rise and demise of world powers.

Likewise, the rapid development of digital technology has revolutionized the way the world approaches international trade. The costs and profits associated with transferring data have skyrocketed as digital technology becomes more affordable and omnipresent. Some figures estimate that the value of European citizens' personal data will grow to nearly €1 trillion annually by 2020.[1] In a highly computerized and digitally interconnected world, not only are goods and services (such as ordering, cataloging, and record-keeping) handled electronically, but the goods and services themselves (software, e-consultation and downloadable products) can be digitally transferred, reducing the time spent between purchase and ownership to an instantaneous click. Today, almost all business transactions, whether they are online or offline, rely on some form of digital management that may come in the form of inventory records, order status tracking information, or employee data. This type of data is transmitted within, between, and among companies, sometimes with the aid of a third party data processor.

While digital technology has facilitated the rise of a number of large-scale and highly profitable technology companies, the plethora of digital management options have also made it easier, faster, and cheaper for small and medium-sized enterprises (SMEs) to operate on a daily basis and eventually scale their businesses to reach a larger customer base. When top-level legislative agreements are scrutinized and even invalidated, SMEs are the hardest hit. For example, when a European court struck down the EU-US Safe Harbor Agreement in 2015, it doomed thousands of American businesses into legal limbo for several months as SMEs struggled to determine whether or not their business practices that involved sending, processing, or storing data on EU citizens were illegal.

The speed of data transfers across the Internet continues to increase. As companies and individuals develop even faster and more efficient ways of facilitating international digital transfers, the need to agree on a uniform method of regulating the countless number of cross-border data transfers becomes even more pressing. The debate over how to regulate international data transfers brings with it a host of other salient topics that are important to consider, such as how to store, process, and access large volumes of data from anywhere in the world. This paper will focus on European data legislation and how data privacy and transfer standards in countries like Turkey and the United States measure up to them.

1 http://europa.eu/rapid/press-release_MEMO- 15-3802_en.htm

WHAT ARE TRANS-BORDER DATA TRANSFERS?

Every time a credit card is swiped at a store, a plane ticket is purchased, or a GPS navigation device is used, personal data is transferred. As everyday transactions in business, politics, and our personal lives become increasingly dependent on digital technology and the Internet, our personal information becomes more widely available and, therefore, increasingly vulnerable. Giving away personal information like full names, birthdates, addresses, and phone numbers to unknown third parties has been normalized to the point where we no longer think twice about volunteering our personal information when prompted to online. Whenever someone creates an account on a social networking website or downloads a messaging app onto their smartphone, they are not only sharing private information with the people they connect with but also giving companies' the right to store and use their private information as outlined in their user terms and conditions.

Companies engaged in cross-border data transactions transport data from one point to another, often using multiple nodes of data transit points scattered throughout the world to relay the information in the process. The Internet automatically locates and funnels data through the closest available data node, switching directions and transferring packets of data in seconds. These data nodes are located in different countries and are shared by Internet users all over the world. Because origin and destination points are scattered across every corner of the globe, one single piece of legislation cannot account for all the necessary measures that need to be in place in order to enforce the protection and privacy of transferred data. However, having disjointed or overlapping legislation, especially when dealing with an issue with drastic international repercussions, further exasperates the already difficult problem of trying to figure out a way to deal with the novel challenges of handling data and emerging digital technologies.

WHY DO COMPANIES STORE DATA?

The safe and secure storage of data is just as important as the safe and secure transfer of data. As data travels from Point A to Point B, data handlers must also ensure that personal data stays private before, during, and after the transfer. Recently, a hacking attack published the personal information of about 50 million Turkish citizens, more than half of the country's population, exposing national identification numbers, addresses, and phone numbers, which the Associated Press verified.[2] Although the highly sensitive nature of Turkish national ID numbers, the equivalent of US social security numbers, should have raised more than a few eyebrows within the Turkish government, members of the Turkish government tried to downplay the gravity of the data breach and instead seemed to chide journalists reporting on the hack instead.[3] In the words of Binal Yildirim, the Turkish Transportation, Communication and Maritime Affairs Minister, "This is a very old story. A similar allegation was made in 2010. The issue is brought to the agenda from time to time. It is now being served like a new story. These outdated reports are not newsworthy."[4]

These unconcerned reactions by the government often mislead the general population about the dangers of data privacy breaches. By downplaying the severity of the consequences of privacy violations, average citizens remain unaware of how rampantly and frequently their personal data is exposed. In addition, people do not fathom how much they rely on digital technology to go about their daily lives. Perhaps, because of this lack of awareness, people are generally loath to organize and demand greater privacy protections from their political leaders.

There are numerous sectors that illustrate how vital data transfers are for business and personal health. One key sector is that of digital medical devices, which store personal and health data for diagnostic and treatment purposes. For example, devices that are too large to transport for repairs and maintenance need to be accessed by authorized repair personnel remotely, gaining access to the personal and health data of patients who depend on these medical devices. Storing such sensitive information about patients is often viewed with suspicion as the engineer or repair crew handling medical device repairs are usually not legally authorized to access such sensitive data.

In more extreme cases, patient data can be leaked or sold to the pharmaceutical industry for marketing and research. Such an extreme case in Turkey was recently covered by the press, whereby Turkish Social Security Institution (SGK) sold a large volume of personal medical data stored in the Medical Tracking System, the centralized state database on medical dose and coverage of patients, to a private pharmaceutical company called Datamed, which belonged to a former member of parliament. Although the legal case was rejected by the court, the evidence provided to the court, namely the Court of Auditors audit report, validated the sale of medical data to private third party companies.

Another controversial sector pertaining to the storage of and access to sensitive data is the energy sector. International Oil and Gas Companies (IOCs) collect and store geographic and geopolitical data on a large

2 https://www.wired.com/2016/04/hack-brief- turkey-breach- spills-info-half-citizens/

3 https://www.theguardian.com/technology/2016/apr/04/database-allegedly- containing-id- numbers-of-50m-turks- posted-online

4 http://www.hurriyetdailynews.com/turkish-minister- calls-massive-data-leak- report-an- old-story.aspx?PageID=238&NID=97321&NewsCatID=341

number of pipeline, upstream, and downstream facilities in order to optimize their exploration, extraction, and export operations. The ability to conduct proper assessments requires storing and processing data on topography, climate, politics (i.e. cases of riot, attack or sabotage), and key technical data that belong to other countries. This begs the question of whether such key strategic data should be accessed or stored by private companies and how privacy protection safeguards can prevent these companies from selling such information to other third parties or foreign intelligence agencies that originally were not the intended recipients of such data.

Similar debates occur in the insurance sector, where foreign insurance companies store and process the data of beneficiaries in other countries. Insurance companies usually cite the need to back up beneficiaries' personal data in a secondary location abroad to ensure efficient processing of data and the physical protection of the data. In other words, if indigenous data centers are harmed physically, such as through natural disasters like hurricanes and tornadoes, data redundancy ensures that copies of the same information are readily available to access at other locations.

These and many more cases of data processing and storage brought about the need for governments to step in and establish certain rules and regulations. Such intervention served two purposes: one, to protect citizens' privacy, and two, to protect sensitive national data that may be defined as 'strategic data.' The debate on restriction versus freedom of data flows is polarized along two lines. The first is that governmental restrictions are necessary to prevent abuse and mishandling of such data, preventing privacy abuses and ensuring protection of sensitive strategic data. The second is that excessive governmental restrictions on data flows impair business speed – just like how high tariffs and excessive border controls stifle trade – and hurt a countries' business competitiveness. Indeed, companies that feel too much intrusion into their handling of data will be inclined to move their businesses to countries where they have more conducive environments in terms of collecting, processing, and storing data. To that end, restrictions on data flows have a direct impact on business and investment.

	Definition	Main Arguments	Criticism
Data Localization Requirements	A government's legal criteria on foreign and/or private companies to either build and use local data storage and processing infrastructure, or stop data collection and transfer altogether. This implies building domestic data centers and indigenous data processing staff.	• Data localization will protect domestic industry • Establishment of domestic data centers will create jobs • Data localization will improve security of data • Data localization will benefit domestic business • Following the recent increase in debates regarding foreign spy agency access to global data flows, it is necessary to localize and nationalize data.	• It will reduce business competitiveness. Force companies to relocate elsewhere • New data centers are expensive and it takes a long time to train efficient personnel. Lack of personnel training will cause mishandling of data more frequently. • Physical location of data is not relevant to security. Regardless of location, a data center needs to be maintained with the most advanced security personnel and infrastructure. • Data localization will only benefit domestic businesses that conduct business domestically. Data localization will impair and raise the costs of domestic enterprises that are doing business with international companies, rendering it another form of protectionism. • Localized data can still be accessed by intelligence organizations. What matters is how efficient and high-tech these data centers are, regardless of where they are physically based. Plus, laws on commercial data transfers are different than law enforcement access to the same data. Restricting commercial data flows doesn't necessarily prevent surveillance.
Privacy Regulations	More detailed and complex set of laws and regulations that aim to protect privacy and minimize abuse, without imposing localization requirements.	• Rather than restricting data flows and slowing business transactions, privacy regulations seek to establish a middle ground between surveillance and ease of business. • Privacy regulations make it easier for authoritarian governments to do business with international companies	• Hard to form an internationally-accepted law on privacy regulations as each country's understanding and practice of privacy is different. • International companies may find it harder to do business in countries with elaborate privacy regulations as these companies have to pursue a different business law in every country.

THE ROLE OF GOVERNMENT IN DATA PRIVACY PROTECTION

Private companies are not the only ones that may abuse or mishandle personal data of citizens. Perhaps an even more important question is how much personal data governments should collect, store, and process on their citizens and what kind of legal precautions should be taken to protect privacy. In order to render citizenship services, bureaucracy, and security more efficient, governments have also begun collecting, storing and processing citizens' personal data, such as address, national identity, financial, and legal background information.

The rationale, scope, and legal framework for data collection are widely disputed among countries. However, many also wrestle with whether countries that lack the sufficient technical infrastructure to protect citizens from cyberattacks should be collecting personal data on their citizens in the first place. For example, in February 2016, the hacker group Anonymous released a large database under Turkey's General Directorate of Security, intending to punish the Turkish government for its human rights abuses. The 18 gigabytes of data that was subsequently released contained a substantial volume of personal data on Turkish citizens as well.

One of the oldest debates in politics, freedom-versus-security, is perhaps more relevant today in the debate between government surveillance versus individual privacy. Since the 1990s, a growing number of countries have adopted data protection and privacy laws or regulations, although commonly shared definitions for personal data, data collection, and data processing differ, rendering these laws incompatible and geared towards disparate outcomes. An important analytical problem arising from these differences is how to approach the issue of data collection. How much data should be collected by the governments and private companies and which legal and ethical constraints should be imposed upon them to prevent collection and processing abuses?

Moreover, who does data belong to? Governments, companies, even computer games collect and store personal data, which in turn, can be accessed, processed, and stored surreptitiously by government surveillance agencies. While the digital age has brought about new freedom frontiers and liberty zones for citizens, it has also provided governments with better tools to respond positively or negatively to the growing scope of electronic liberties. The emergence of multiple data collection bodies and institutions and their overlapping and sometimes competing data storage policies bring in the question of what happens if personal data is lost, damaged, or misused? Although countries approach this question individually, as is their sovereign right, data ownership is usually divided between three legal fronts: copyright, confidentiality, and contract. Data copyright implies intellectual property, assigned automatically to the creator, and prevents unauthorized copying and publishing of an original work. Data confidentiality is defined by the United Nations Economic Commission for Europe (UNECE) as 'a property of data, usually resulting from legislative measures, which prevents it from unauthorized disclosure.[5] Finally, a data contract, as defined by Microsoft, is 'a formal agreement between a service and a client that abstractly describes the data to be exchanged. A data contract precisely defines, for each parameter or return type, what data is serialized (turned into XML) to be exchanged.'[6]

5 http://www.eqavet.eu/qa/gns/glossary/d/data-confidentiality.aspx

6 https://msdn.microsoft.com/en-us/library/ms733127(v=vs.110).aspx

Regardless of the source or purpose of the stored data, emerging markets like Turkey must align their data protection legislation with the standards of their trading and political partners. As a European country and aspiring EU member, Turkey must shape its laws to fit the mold of Europe. With the Law on the Protection of Personal Data newly ratified by parliament, Turkey is starting to take steps toward reforming its outdated or nonexistent data protection laws to better respond to the challenges of the 21st century.

HOW ARE TRANS-BORDER DATA TRANSFERS REGULATED?

A mix of international, regional, and national legislation regulates data transfers within and across international borders. Perhaps the most notable piece of legislation is the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (1980). The OECD Guidelines were the first international attempt at tackling the issue of data privacy, guaranteeing privacy rights to individuals and contains details on the collection, processing, and dissemination of data for international data transfers.[7] "Principle-based and technology-neutral," the OECD adopted the guidelines after recognizing the importance of personal information in the global economy and over concerns of the potential impact of emerging computer technology.[8]

For over a decade, the European continent specifically has adopted a number of regulatory mechanisms to address the issue of data privacy and data transfers, which arguably are the most stringent of privacy protection measures existing today. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) was the first binding international instrument that protected individuals against abuses accompanying collection and processing of personal data. As the Convention's summary states, "This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data … In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of 'sensitive' data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards."[9]

Then, in 1995, the EU Data Protection Directive went into force, setting up "a regulatory framework which [sought] to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union."[10] The Directive protects data subjects, or the people whose personal data are being processed, from unlawful and unfair use of their personal data. Data subjects are allowed three rights: the right to obtain information, the right of access, and the right to object. These rights gave EU citizens the right to obtain information about their own personal data being processed by data controllers, the right to access their own personal data, and the right to formally object when they felt that their personal data was being processed unfairly and unlawfully. The Data Protection Directive allowed Member States to transfer personal data to a third country with an "adequate level of protection."[11]

In addition, the European Charter of Fundamental Rights (2000), legally binding to all EU member

7 http://www.oecd.org/sti/ieconomy/49710223.pdf pg. 3

8 http://www.oecd.org/sti/ieconomy/49710223.pdf

9 Council of Europe, "Details of Treaty No.108" http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

10 "Protection of Personal Data," European Union, accessed 18 April 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012

11 Ibn al.

states, specifically protects rights to privacy, data protection, and effective judicial remedy in the case of wrongdoing. After the Lisbon Treaty went into effect in 2009, data protection became a fundamental right, further cementing European privacy laws against government proclivity for loosening privacy protection mechanisms in favor of more invasive security measures.

In 2000, the EU and the US agreed on the Safe Harbor Agreement, which provided the "adequate level of protection" necessary for data to be legally transferred between EU Member States and the US. Given the crucial political and economic alliance between the United States and the European bloc, this agreement served as a vital method for thousands of American and European businesses to legally export data on European citizens to the US. Aspiring to become a single digital market, the EU negotiated the Safe Harbor Agreement to serve as a "one stop shop" for companies to get information on how to conduct data transfers in line with EU laws.[12]

After the National Security Agency government leaks in June 2013, however, the US and its companies came under great scrutiny after the leaked documents showed evidence of ongoing mass government surveillance programs. Among the documented surveillance activity, several instances of the US spying on close European allies like Germany and the United Kingdom emerged. In response, the European Court of Justice invalidated the Safe Harbor Agreement in October 2015, citing that it did not provide adequate privacy protection for the 500 million citizens of the European Union. The ensuing uncertainty left over 4,000 American and European businesses in the dark on whether they could continue transferring data on their clients and users from Europe to the US.[13]

For the next two years, European and American privacy experts and lawmakers negotiated the terms of a revised data privacy agreement that would serve a similar function to the Safe Harbor Agreement, albeit with a few additions. In February 2016, the Article 29 Working Party, a group of data protection authority representatives from all 28 EU Member States, presented the EU-US Privacy Shield Agreement that would serve as the new standard upon which EU citizen data could be exported to the US.

Two major provisions exist in the Privacy Shield Agreement that European leaders felt were not sufficiently guaranteed in the now defunct Safe Harbor Agreement. The first was greater limitations placed on US intelligence agencies regarding the collection of personal data in intelligence gathering operations. Because the NSA leaks showed that the US was spying even on close allies in Europe such as Germany, public outcry against government surveillance reverberated throughout the European continent, leading the countries' leaders to call for stricter measures to protect EU citizens against the US's intelligence gathering operations. The Office of the Director of National Intelligence explicitly assured in Privacy Shield "that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms, preventing generalized access to personal data."[14]

The second major addition to the Privacy Shield Agreement was a formal system of judicial redress for EU citizens who felt that their personal data was being improperly handled. First, the US government will create an independent ombudsman within the Department of State who "will follow-up complaints and enquiries by individuals and inform them whether the relevant laws have been complied with."[15] Companies

12 https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court- declare-invalid-data-protection

13 http://www.nytimes.com/2015/10/07/technology/european-union- us-data- collection.html?_r=0

14 http://europa.eu/rapid/press-release_IP- 16-433_en.htm

15 Ibn al.

must resolve complaints received from EU citizens within 45 days. If not, EU citizens have the right to go directly to their national data protection authorities, who will then work with the US Federal Trade Commission to investigate and resolve privacy protection complaints. All of these mechanisms of judicial redress will come at no cost to the individual filing the complaint.

To further ensure that the Privacy Shield Agreement stays up to date, the European Commission, the US Department of Commerce, and national intelligence experts from the US and European Data Protection Authorities will conduct annual reviews to ensure that the existing agreement sufficiently protects EU citizens without obstructing the work of law enforcement and national security agencies. Moreover, annual privacy summits with relevant NGOs and other stakeholders will be held "to discuss broader developments in the area of U.S. privacy law and their impact on Europeans."[16]

In lieu of the EU-US data transfer agreements, however, companies could still continue business as usual through other means, such as through binding corporate rules (BCRs) and model contractual clauses (MCCs). Binding corporate rules are "internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection."[17] In other words, they are company-specific arrangements that allow for the transfer of data from Europe to countries like the United States according to the principles laid out in the Data Protection Directive of 1995.

Additionally, the EU affords two sets of standard contractual clauses for data transfers from EU data controllers to non-EU data controllers and for data EU data controllers to non-EU data processors.[18] However, because BCRs and MCCs are so time-consuming and costly, only big companies with substantial resources are able to use them. For this reason, it is usually small- and medium-sized businesses that are most disadvantaged by the invalidation of agreements like Safe Harbor and Privacy Shield.

THE FUTURE OF DATA TRANSFERS IN EUROPE

A number of ongoing negotiations and revised legislation are in the pipeline in Europe. In December 2015, the European Commission, European Parliament, and European Council agreed upon the General Data Protection Reform, which unified fragmented legislation across different countries and sectors into a single legal framework that would form the basis of European data protection regulations if formally adopted.[19] The reform is comprised of the General Data Protection Regulation and the Data Protection Directive and took three years of negotiations over its wording and content. The European Council and the European Parliament then formally adopted the updated version of the Regulation and Directive in April 2016, and both will go into effect two years later in 2018.

The Reform gives law enforcement agents one single reference point to access and protect the data of victims, witnesses, and suspects in criminal investigation cases. Phil Lee, a law firm partner at Fieldfisher familiar with European data protection laws, said, "This is the most significant development in data pro-

16 Ibn al.

17 http://ec.europa.eu/justice/data-protection/article- 29/bcr/index_en.htm

18 http://ec.europa.eu/justice/data-protection/international- transfers/transfer/index_en.htm

19 European Commission, "Agreement on Commission's EU data protection reform will boost Single Digital Market," 15 December 2015, http://europa.eu/rapid/press-release_IP- 15-6321_en.htm

tection that Europe, possibly the world, has seen over the past 20 years. Forget Safe Harbour and Right to be Forgotten – this is much, much more significant."[20] Furthermore, in an effort to give Europeans better control over their own personal data, companies are now required to notify individuals when their data has been hacked and must grant a "right to be forgotten" for European citizens under the new reform.[21] This meant that when EU citizens no longer wanted their data to be processed and no legitimate grounds for retaining their personal data existed, the data specified would be deleted.[22]

A much-needed push to consolidate data legislation and information, the General Data Protection Reform also addresses data privacy in relation to small and medium enterprises (SMEs). Because the Reform applies to all 28 EU member countries, the streamlined and easy-to-access data privacy laws are aimed at facilitating cross-border trade and economic development. EU Commissioner for Justice, Consumers and Gender Equality Vera Jourova said, "Citizens and businesses will profit from clear rules that are fit for the digital age, that give strong protection and at the same time create opportunities and encourage innovation in a European Digital Single Market. And harmonized data protection rules for police and criminal justice authorities will ease law enforcement cooperation between Member States based on mutual trust, contributing to the European Agenda for Security."[23]

The Privacy Shield Agreement is pending official adoption. After the Privacy Shield Agreement was announced in February 2016, the Article 29 Working Party, the group of data protection authorities from all 28 EU countries, examined the agreement for two months before releasing their opinion in April. Regarding the Privacy Shield Agreement as it is, they applauded the improvements made to the agreement compared to Safe Harbor but still cited concerns over bulk intelligence collection programs and the independence and efficacy of the ombudsman.[24] Although the group's opinion is not legally binding, they still hold great influence over European legislators who will have to make a decision on whether or not to adopt the Privacy Shield Agreement in the coming months.

TURKEY'S DATA REGULATIONS

Turkey's data protection legislation negotiations with the European Union began in 2003, when the EU Accession Partnership Document first emphasized the matter as a prerequisite for membership. Although adopting this criterion into the EU Accession National Programme, Turkey did not pursue the matter and draft legislation. The issue re-emerged in 2014, largely out of the need to co-operate with the EU legal and police institutions EUROJUST and EUROPOL, following the intensification of the Syrian refugee crisis. In addition, the EU 2013 Progress Report had criticized the lack of a dedicated data protection law in Turkey that would enable better cooperation between Brussels and Ankara. A specific source of criticism was that Turkey had adopted a Cyber Security Council and a National Cyber Security Strategy and Action Plan, yet had taken no steps on the protection of personal data and e-commerce regulations.

The December 2014 'Draft Law on the Protection of Personal Data' along with its revised 2016 version

20 https://www.theguardian.com/technology/2015/dec/16/eu-agrees-draft-text- pan-european- data-privacy-rules

21 European Commission, "Questions and Answers: Data protection reform," 21 December 2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

22 http://europa.eu/rapid/press-release_MEMO- 15-3802_en.htm

23 European Commission, "Agreement on Commission's EU data protection reform will boost Single Digital Market," 15 December 2015, http://europa.eu/rapid/press-release_IP- 15-6321_en.htm

24 http://uk.businessinsider.com/article-29- working-party- verdict-on-privacy-shield- data-transfer-mechanism-2016- 4

have been analyzed in depth in a previous EDAM Report.[25] EDAM's main criticism of both versions of the draft law was the fact that the proposed Data Protection Council would be substantially short of fulfilling the requirements of independence and would effectively be a political – rather than technical – body. Furthermore, the draft law had too many exceptions to the limit of the government's collection, processing and storage of personal data, effectively falling substantially short of a reform document.

Before the proposed 'Draft Law on the Protection of Personal Data', there were several existing laws that refer to the collection and use of such data. Primarily, the Turkish Constitution, following the amendments of 2010, has rendered the protection of personal data a part of individual rights, introducing restrictions to the state's ability to record and process such data. Such specific Articles of the Constitution are 17 (general acknowledgement of the individual's right of 'living, protection and improvement of his material and spiritual being') and 20 (acknowledgement of the right to 'request the protection of data', including correction and deletion of such data). In Turkish Civil Code on the other hand, Articles 23, 24 and 25 guarantee personal rights, although those that are not specific to online identity or data rights. The Code of Obligations (Law 6098) refers mostly to the financial aspect of data use, as its Article 419 renders employers responsible of their employee's personal data on performance and qualifications. Finally, the Criminal Code Articles 134 (violating secrecy of private data), 135 (illegal recording of data, violation of data collection law, data collection without consent), 136 (transfer and dissemination of personal data) and 138 (data deletion policy and failure in deletion). In addition, the Law on the Right to Access Information allows a degree of access to certain institutional, personal and governmental data, with explicit restrictions on secret data.

There are also sector-specific laws on data protection such as Regulation on Procedures and Principles of Broadcasts via Internet and Regulation on Mass Internet Use Providers, the Ecommerce Law, Regulation on Protection and Sharing of General Health Insurance Data, Regulation on Data Privacy and Principles and Procedures Regarding Security of Confidential Data in the Official Statistics, Regulation on Bank Cards and Credit Cards, Regulation on Distance Contracts and the Electronic Communications Law and its secondary legislation.

From the point of view of companies that are entering or already operating in the Turkish market, several additional data protection laws should be considered:

- Labor Law #4857, Article 75 makes it necessary for the employer to keep 'any data necessary' in addition to employees' identification information. The law necessitates the disclosure of such data to law enforcement agencies, but restricts their use outside of 'rules of honesty' and within legal requirements.

- Banking Law #5411 as well, necessitates disclosure of clients' personal data to law enforcement agencies only, restricting the use of such data in any other form. The Banking and Credit Card Law #5464, Article 23 follows up by clarifying cases when credit card data can be processed. The Article indicates that in addition to law enforcement agencies, other institutions and agencies that are explicitly mentioned in the law (widest understanding of all available laws) can also access such information.

- Medical Deontology Code, Article 4 specifies that personal data can be used and processed only to the extent required for medical practice and not for the purposes of research dissemina-

25 http://edam.org.tr/en/File?id=3187

tion, such as conferences or articles. Even in cases where the patient waives any claim on medical data, the Code prohibits transfer of such data.

- Electronic Communications Law #5809, Article 4 focuses on the transfer of data and brings in the necessity of protecting data security and confidentiality of electronic communications. In addition, this law enables Information and Communication Technologies Authority (BTK) to produce new regulations with regard to processing and storing personal data. However, following successive appeals from the Constitutional Court and the Council of State, BTK was stripped of its legal right to process personal data, citing incompatibility with the Constitution. In addition, the Legislation on the Processing and Protection of Personal Data in Electronic Communications Sector, that was put into effect in January 2013, harmonizes the issue of protecting personal data in line with the EU's 2002/58 legislation, with a specific focus on Internet Service Providers.

- Electronic Signature Law of #5070 regulates the processing of personal data in digital certificate platforms. A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate. The Law #5070 restricts the collection of personal data only to enable the processing of a digital certificate, and prohibits storing such data in a way that becomes accessible by third parties.

TURKEY'S COOPERATION WITH EUROJUST AND EUROPOL

Eurojust and Europol are two European Union institutions that handle judicial and police co-operation on crime and criminal surveillance and intelligence. Formed in 2002 and 1998 respectively, Eurojust and Europol aim to crack down on trans-border criminal networks and are crucial for Turkey with regard to cooperation against smuggling, drug trafficking, and human trafficking issues. In January 2008, for example, Europol, Eurojust, and the Turkish police cooperated in Operation Greensea, cracking down on a Turkish/Chinese smuggling gang that was trafficking large numbers of Turks of Kurdish origin into the UK, arresting 23 people in France, Belgium, and the UK. In addition, Europol-Eurojust cooperation with Turkey is critical as Turkey is a key heroin trafficking route from Afghanistan and Pakistan into the EU. On Turkey's end, drug trafficking is a major security issue, as funds from such sources yield substantial revenues for the outlawed Kurdistan Workers' Party (PKK). Coordination with these two European institutions is key for Ankara to monitor, track, and extradite individuals taking part in PKK funding and recruitment operations in Europe.

However, a pressing necessity to hasten and expand this cooperation emerged with the intensification of the Syrian refugee problem. EU Council Report indicates that 'Following reductions in departures from Libya and Western Africa, Turkey is now the principal transit country for illegal migration to the EU. Irregular migrants transit Turkey en route to Greece, Bulgaria and Cyprus, with Greece the main entry point into the EU for onward travel to other Member States, including Italy. FRONTEX assesses that Greece now accounts for 75% of all detections of illegal border-

crossings in the EU.'[26] Both the sheer size of the refugee crisis and their exponential effects on existing smuggling and criminal issues in Turkey and the EU, have forced Turkish and European police and justice institutions to work closer. This was the rationale, when the EU 2013 Progress Report underlined the necessity of a dedicated personal data protection law in Turkey, to make such cooperation legally possible.

Although Turkey responded to this call with its 2014 Draft Law on the Protection of Personal Data and had later revised it based on commentary by European and Turkish legal observers, the updated 2016 version falls even shorter to meet EU standards. In early March 2016, Eurojust prepared a report, indicating that legal cooperation with Turkey on the refugee issue would be very difficult within existing legal structure in Turkey. To that end, the report warned against signing the most recent refugee deal with Ankara, arguing that it didn't have necessary infrastructure to enforce or monitor the terms in the agreement.

26 http://www.statewatch.org/news/2010/aug/eu-council- eurojust-europol- frontex-int-sec-9359- 10.pdf

CONCLUSION

On April 14, 2016, EU lawmakers approved a law that allowed the easier exchange of airline passenger data among the national security forces in EU Member States. In light of terrorist attacks that have rattled European capitals like Paris and Brussels, European citizens and lawmakers have pushed for measures that would better facilitate the transfer of sensitive data. Although the law regulating the retention and transfer of passenger name records (PNR) – which includes name, travel dates, itinerary, ticket details, contact details, travel agent, means of payment, seat number, and baggage information – had been "stalled" in parliament, the growing urgency to update existing data privacy and transfer laws to conform to contemporary problems and the rising fear of more terror attacks from returning jihadists have pushed the normally privacy-centric European continent to more aggressively find ways to utilize personal data effectively and fairly.[27]

Spurred by similar motivations, Turkey adopted the Law on the Protection of Personal Data. Although it has made strides in attempting to address the issue of data privacy and transfers in the last few years, the country still has a long way to go in order to adequately to protect its citizens and the citizens of European partners. With the aim of institutionalizing a more robust data protection regime, Turkey should take note of the number of European legislative efforts that more adequately safeguard citizens from the misuse and abuse of personal data.

27 http://www.reuters.com/article/us-eu-security-airlines-idUSKCN0XB1AG

ABOUT THE AUTHORS

Asst. Prof. H. Akın Ünver

Board Member, EDAM
Faculty Member, International Relations,
Kadir Has University

Akin Unver is an assistant professor of International Relations at Kadir Has University, specializing on energy politics, conflict psychology and radicalization sociologies. In addition, he studies discourse theory, Regional Security Complex Theory and psychoanalytical approaches to decision-making and teaches courses on Politics of the Middle East, Diplomatic History, Energy Security (graduate-level) and Security Theory (PhD-level). A graduate of Bilkent and Middle East Technical Universities, Dr. Unver completed his PhD at the University of Essex, Department of Government. Dr. Unver was a Marcia Robins - Wilf Young scholar at the Washington Institute for Near East Policy in 2007-08 and a dual post-doctoral research at the University of Michigan's Center for European Studies and the Center for Middle East and North African Studies in 2008-2010. He was awarded the position of Ertegun Lecturer at the Princeton University's Near Eastern Studies Department, teaching courses such as History of the Middle East, Conflict-Terrorism Sociology and Turkish Political Sociology - he was also the first scholar to retain the Ertegün chair for two consecutive years at Princeton. Having published in Foreign Affairs, The Diplomat, Columbia Journal of International Affairs, Middle East Quarterly, Middle East Policy and Yale Journal of International Affairs, Dr. Ünver has also spoken and lectured at invited events at Princeton University's Woodrow Wilson School, Georgetown University's Edmund Walsh School of Foreign Service, London School of Economics' Middle East Center and Woodrow Wilson International Center for Scholars. He regularly appears for commentary on BBC World News, France 24, Finnish National Broadcasting Company and Al Jazeera International.

Grace Kim

Research Assistant, EDAM

Grace Kim graduated from Princeton University's Department of Politics in 2013 with a minor in Near Eastern Studies. Upon graduation, she was awarded a U.S. Student Fulbright Fellowship to conduct research on the intersection of politics, law, society, religion, and the economy and its influence on women's rights in Turkey. She is currently working as a research assistant at EDAM, where she focuses on foreign policy and security issues.

Centre for Economics and Foreign Policy Studies

edam

EDAM Cyber Policy Paper Series 2016/3

June 2016

Cross-Border Data Transfers and Data Localization

Asst. Prof. H. Akın Ünver
Board Member, EDAM
Faculty Member, International Relations, Kadir Has University

Grace Kim
Research Assistant, EDAM