Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr
Cilt: 1, Sayı: 2
Geliş: 14.10.2019
Kabul: 12.12.2019

Privacy Impact Assessment as a Tool for GDPR Compliance Preparation

Bilgin, Metin
Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Bölümü, İstanbul, Türkiye, bilgin.metin@boun.edu.tr
ORCID: https://orcid.org/0000-0002-5828-9770

Sema, Erkan
Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Bölümü, İstanbul, Türkiye

İdil, Atasu
Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Bölümü, İstanbul, Türkiye

Enes, Yılmaz
Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Bölümü, İstanbul, Türkiye

ABSTRACT
Technology allows individuals and enterprises to share and disseminate their personal financial, legal, and reputational data via various tools. Such usage may cause loss of control over personal data. The protection of personal data is an indispensable obligation of companies. Eventually, Laws on Protection of Personal Data were enacted by parliament in Europe, such as firstly European Union (EU) Directive 95/46/EC and later General Data Protection Regulation (GDPR). Turkey also adopted a Personal Data Protection Law that was based on EU Directive 95/46/EC on 7 April 2016 as part of its efforts to complement its legislations with the EU. The Turkish Data Protection Law (TDPL) has been leaning more toward the GDPR. European Enterprises and their international business partners should comply with GDPR. In GDPR compliance, Privacy Impact Assessment (PIA) plays an important role. In this literature survey study, the compliance process for TPDL is summarized. Then, how PIA can be utilized as a facilitator for business endeavors for GDPR bound companies is emphasized.

Keywords: *Privacy, Privacy Impact Analysis, Privacy Impact Assessment, Compliance*

GDPR Uyumluluk Hazırlığı için bir Araç Olarak Mahremiyet Etki Değerlendirmesi

ÖZ
Teknoloji, bireylerin ve işletmelerin kişisel finansal, yasal ve itibar verilerini çeşitli araçlarla paylaşmalarını ve yaymalarını sağlar. Bu kullanım kişisel veriler üzerinde kontrol kaybına neden olabilir. Kişisel verilerin korunması, şirketlerin kaçınılmaz bir yükümlülüğüdür. Sonunda, Kişisel Verilerin Korunması Hakkında Kanunlar, Avrupa Parlamentosu tarafından ilk önce 95/46 / EC sayılı AB Direktifi ve daha sonra Genel Veri Koruma Yönetmeliği (GDPR) adları altında kabul edildi. Türkiye, mevzuatını Avrupa Birliği ile tamamlama çabalarının bir parçası olarak, 7 Nisan 2016 tarihinde, 95/46 / EC sayılı AB Direktifine dayanan bir Kişisel Veri Koruma Yasasını da kabul etmiştir. Türkiye Veri Koruma Kanunu (KVKK), zaman içinde GDPR'a daha fazla yönelmiştir. Avrupalı İşletmeleri ve onların uluslararası iş ortakları da GDPR'a uymalıdır. GDPR'a uygunluk surecinde, Gizlilik Etki Değerlendirmesi (PIA) önemli bir rol oynar. Bu literatür çalışmasında KVKK için uygunluk süreci özetlenmiştir. Daha sonra ise, PIA'nin GDPR'a bağlı şirketler için ticari çalışmalar açısından ne şekillerde kolaylaştırıcı olabileceği vurgulanmaktadır.

Anahtar Kelimeler: Mahremiyet, Mahremiyet Etki Analizi, Mahremiyet Etki Değerlendirmesi, Uyumluluk

Atıf Gösterme	Metin, B., Erkan, S., Atasu, İ. ve Yılmaz, E., (2019). Privacy Impact Assessment as a Tool for GDPR Compliance Preparation, *Kişisel Verileri Koruma Dergisi.* *1*(2), 75-86.

INTRODUCTION

The data protection concept is related to both individuals and enterprises. As the technology evolves and constitutes an essential tool in our lives, we are spending most of our time on the Internet surfing in e-commerce or entertainment sites and allowing enterprises to collect significant personal data such as our credit card numbers, GSM numbers, detailed address and IP address. Personal data means any information connecting to an identified or identifiable real person (Wright & Hert, 2012). In this respect, the name, surname, vehicle plate, official address, telephone number, closed-circuit camera images, voice recordings, fingerprints or genetic information of a person are examples of personal data.

There are various definitions of data. Whitney states that data is the basic building block that, when arranged in different ways, becomes information, which can become practical knowledge and even wisdom (Whitney, 2012). Tuomi, sees data as “simple facts” that are waiting to become information. Furthermore, using artificial intelligence, data may be transferred into meaningful information from which knowledge can be retrieved (Tuomi, 1999). In summary, data is the smallest element of knowledge that could bring us to the wisdom stage in the end.

Acquisti states that the privacy and protection of personal data has several dimensions. One is the economic dimension. The protection of the individual’s psychological and physical well-being can be interpreted in economic terms as sources of an individual’s utility (Acquisti, 2010) which the rational individual is expected to maximize in economics. In terms of market dynamics, Calzolari and Pavan find that the unrestricted sharing of consumers' personal data between two firms may in fact reduce market distortions and increase social welfare, including that of the consumers’ (Calzolari & Pavan, 2006).

As big data evolves nearly in every sector, personal data turns out to be an issue for companies. Since it is difficult to separate personal data from big data, companies try to find out new solutions that obey the legal regulations (Newman, 2008). Mayer-Schönberger & Cukier (2013) declares that big data is getting bigger and messier but also more valuable because the economic system all around the world becomes dependent on big data.

As Zerlang (2017) discusses, one of the greatest misunderstandings in today’s business world is that compliance equates to good business practice – particularly about security. Zerlang (2017) says that compliance ensures a base level of security to which companies must adhere in order to ‘check the box’. Biagini L. (2018) also supports that privacy and security are complementary. Zerlang (2017) asserts that cybercrime is evolving rapidly, so it is often difficult for regulations and legislation to keep up with a changing security landscape.

The EU's General Data Protection Regulation (GDPR) offers an opportunity to cyber-security and compliance which are two areas often seen as disparate by business leaders (Zerlang , 2017). Legal acts are also required to comply with standards. According to Biagini L. (2018), ignoring the differences between compliance and security could be very important, or else security controls only become a box-ticking exercise. Biagini (2018) indicates that “data protection in the GDPR is not a security term. It's more about protecting the rights of individuals over the use of their personal data than it is about securing that data”. In a manner, security and privacy words are supposed to have a similar meaning. However, Siegel (2016) explains the difference between security and privacy in such a way: “Security supplies protection for all types of information, in any form, so that the information’s confidentiality, integrity, and availability are maintained”. In contrast, privacy assures that personal information (and sometimes corporate confidential information as well) are collected, processed (used), protected and destroyed legally and fairly.

In this study, we first explain the components necessary to comply with the Turkish Data Protection Law (TDPL) regarding the protection of personal data and security rules in Turkey. Then we explain how to prepare a Privacy Impact Assessment based on this compliance process.

THE PREREQUISITES FOR COMPLIANCE WITH TDPL

The GDPR replaced the Data Protection Directive 95/46/EC (DPD) presented in 1995 and, being an order, left some space for elucidation amid its transposition into national laws. Politou E., Alepis E., Patsakis C. (2017) asserted that, on 27 April 2016, following four years of drafting, campaigning and negotiations among the EU Member States and many influenced organizations, the EU General Data Protection Regulation (GDPR) has been concurred and concluded, though on 4 May 2016 its last content distributed in the Official Journal of the European Union. Following a two-year execution period, the GDPR has been connected over the European Union from 25 May 2018. The Grand National Assembly of Turkey (TBMM, GNAT) has also accepted the Law on the Personal Data Protection numbered 6698 on 24th March 2016, which is called TDPL. TDPL was published in the Official Gazette on 7th of April in 2016 and has been applicable since 7 April 2018. Also, Turkish Data Protection Authority (TDPA) as an independent authority was formed to supervise and regulate the Turkish market. Therefore, it is essential that enterprises take notice of these laws and regulations. The aim of this section is to shortly describe the important steps for TDPL compliance. Of course, it is impossible to explain the whole compliance process completely in a short section, but useful resources such as Dülger (2016) are already available for this purpose.

(ISMS Policy & Privacy Strategy

Before starting GDPR and/or TDPL compliance process, having an active privacy management cycle as part of an Information Security Management System (ISMS) that includes a managerial and technical dimension is a good starting point. Organizations, which follow specific security standards or/and frameworks, can comply with Data Protection Law in a shorter span of time. If the organization has ISMS, it may already have a security policy that considers the privacy and security strategy that is aligned with its business objectives. Otherwise, it can be very useful to specify a privacy policy and strategy that aligns with the organization's business objectives and The Law No. 6698.

Management Support

Having dedicated resources and top management support are also necessary before and during getting compliance with GDPR and/or TDPL. Compliance with the Law is not a finite project, but it is a living process. Thus, management support and involvement are inevitable for continuous compliance processes. Some researches show that about 70% of all projects fail to meet their objectives (Billows, 2015). As Burger states that 33% of projects fail because of a lack of involvement from senior management, thus it has a vital importance (Burger, 2016).

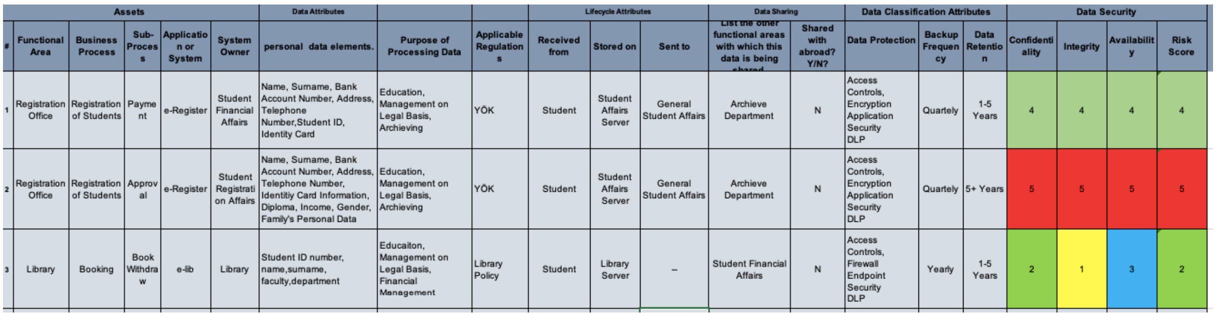
Definition of Organization, Roles & Responsibilities

Firstly, all data controllers must have a correspondent for managing the relations with the TDPA. Also in this stage, the organizational chart of the firm is prepared if it does not exist or if any updates are needed they are done. This chart must also clarify the roles and responsibilities of the departments and people. For the compliance process, the project team is formed in light of some specific circumstances. The experiences of people who manage TDPL compliance in their organizations explain that the project teams should consist of at least one employee from the departments such as audit (if it exists), human resources, information technology and legal. The data controllers should give trainings to their employees for data protection awareness. Besides, they should implement disciplinary sanctions if they act against data protection policies and procedures of the company.

Business Processes

Organizations should have clear interaction processes with all of their operations whether they are daily or quarterly activities. Each department should identify the properties of the data that might comprise of source, destination, purpose, location stored, shared parties and departments and expiration time. The most important action is to decide whether data is needed for operations or not. All of the hard copy, online and even cloud documents should be taken into consideration during that process. For example, legacy systems have too much information dating back to 20 years ago, which are not used in current operations. This is inefficient since it creates difficulties in storage and performance.

Data Inventory and the Risk Value of Data



Assets						Data Attributes			Lifecycle Attributes			Data Sharing		Data Classification Attributes			Data Security			
#	Functional Area	Business Process	Sub-Process	Application or System	System Owner	personal data elements.	Purpose of Processing Data	Applicable Regulations	Received from	Stored on	Sent to	List the other functional areas with which this data is being shared	Shared with abroad? Y/N?	Data Protection	Backup Frequency	Data Retention	Confidentiality	Integrity	Availability	Risk Score
1	Registration Office	Registration of Students	Payment	e-Register	Student Financial Affairs	Name, Surname, Bank Account Number, Address, Telephone Number,Student ID, Identity Card	Education, Management on Legal Basis, Archieving	YÖK	Student	Student Affairs Server	General Student Affairs	Archieve Department	N	Access Controls, Encryption Application Security DLP	Quartely	1-5 Years	4	4	4	4
2	Registration Office	Registration of Students	Approval	e-Register	Student Registration Affairs	Name, Surname, Bank Account Number, Address, Telephone Number, Identitiy Card Information, Diploma, Income, Gender, Family's Personal Data	Education, Management on Legal Basis, Archieving	YÖK	Student	Student Affairs Server	General Student Affairs	Archieve Department	N	Access Controls, Encryption Application Security DLP	Quartely	5+ Years	5	5	5	5
3	Library	Booking	Book Withdraw	e-lib	Library	Student ID number, name,surname, faculty,department	Educaiton, Management on Legal Basis, Financial Management	Library Policy	Student	Library Server	–	Student Financial Affairs	N	Access Controls, Firewall Endpoint Security DLP	Yearly	1-5 Years	2	1	3	2

Figure 1. Data inventory table template on Excel

The inventory table in Fig. 1 consists of assets, asset category, data type, data owner and the risk analysis of those assets. Value of data and risks among data are defined according to data triad "CIA" that stands for Confidentiality, Integrity and Availability. Information Security is based on these 3 measures and risk analysis is always held with this triad. Other metrics like the reputation of the company shall be used when determining the risks of data. After defining the value of data, prioritization of data is done in terms of its importance value. Finally, by multiplying the impact and probability of a risk, the risk value of data is found.

While making risk analysis, the principles written below should be applied:

- A risk management policy should be established.
- Risk management and evaluation procedure should be established.
- It should be ensured that the relevant risks from each department are filled in with the "Personal Data".
- Risk transfer criteria should be determined.
- Risk appetite should be determined.
- Risk processing standards should be determined.
- Probability, volume, impact, threats, risk matrix and action matrix should be defined.

Inventory tables may not have the risk analysis; but Risk Policy should be defined.

Inventory tables when assessing data are mostly filled by the employees of the departments for the reason of their knowledge about their work. They are given a template table and responsibility for the data entry. The importance of workflows and dataflows comes now. Because, predefining the processes and data will help when building Excel tools to prevent user errors.

Legal Process

In the legal process, the business processes carried out within the institution are subject to legal analysis. Legal professionals carry out legal analysis that defines what is to be done about the personal data processed in the daily operations of the business units.

In addition to the data processing inventory, it is important to prepare data processing, retention and neutralization (deletion, destruction or anonymization) policies for lessening personnel data. Also, the legal agreements and forms of the institution are revised and processes such as the creation of obligatory informative and explicit consent texts are also included in the legal stage of the compliance process. Review and improvement of the contracts between employees, stakeholders and third parties are the other responsibilities, which are part of this process.

The major condition for processing data which is "explicit consent" is prepared by the data controller with the consultancy of lawyers. The data controller is obliged to provide the information stated by the personal data protection law and to obtain the explicit direct consent of data subject for processing of his/her data, especially for personal data. Review and improvement of the contracts between employees, stakeholders and third parties are the other responsibilities which held in this process. As mentioned above, the data inventory table has significance within the process because the legal department or consultants make the determination of legal risks and actions for compliance in accordance with the inventory table. Organizations must create a storage and destruction policy, that clearly covers storage environment, shared parties, sharing method and storage period. Finally, data controllers providing special conditions in TDPL have to register with "Data Controllers' Registry".

Technical Process

Turkish Data Protection Authority has published a guideline about the technical and managerial controls which needed to be applied by the companies who process personal data (TDPL, January 2018). It has 6 main specifications related with technical implementations.

- Ensuring cyber security that comprises of patch management, password policy against brute force attacks, antivirus, firewall, access rights and SSL protocol.
- Tracking personal data security that encompasses vulnerability analysis, penetration test, logging, SIEM, IDS/IPS Reports
- Ensuring security of personal data environments that contain physical security, password management, e-mail security, encryption, AES, mobile device usage limitations
- Storage of personal data in the cloud which requires service provider analysis, synchronization, back-up, two-factor-authentication.
- Information technology systems supply, development and maintenance requirement analysis, SLA (Service level agreement), third party contracts.
- Backup of personal data that includes periodical controls on back-up systems against ransomware.

Monitoring

Even if all the organizational, legal and technical processes are implemented, it does not mean that the compliance is over. Since it is a continuing process, it must be controlled and monitored continuously. Because data on hand changes from time to time and there is no security for the system against novel threats, it must be updated if there are any changes. Data subjects have rights to know how their data is processed, to request deletion and upgrade and compensation if any damage occurs. Thus, explicit consents of each data subject must be stored in a database in the case of a cancellation request. All the policies, diagrams and data inventory tables must be updated after any changes in the operation, consents, strategies or tools. The perfect way of managing this requirement is training. Employee training is a must from head to toe in the compliance process as in all the operations of an organization.

PRIVACY IMPACT ASSESSMENT

PIA plays an important role in data protection and privacy literature. For example, Binn wrote that 'PIAs could be seen as an evolution of provisions set out in early data protection regimes in which organizations were required to register, notify, and check with national authorities to ensure compliance prior to processing' (Binn, 2017). Article 20 of the European Data Protection Directive of 1995 institutionalized 'prior checking' and notification with a national authority. Then some academic studies presented in the literature entitled with 'privacy impact analysis such as (Flaherty, 2000). Later guidance studies on conducting PIAs were published by some national privacy and data protection authorities or commissions such as International Commissioner's Office (ICO) from the UK and the Securities and Exchange Commission (SEC) from the US (ICO, 2015, SEC, 2007). Eventually, Article 35 of the GDPR requires organizations to conduct impact assessments prior to personal data processing that may result in a high risk to the rights and freedoms of natural persons (GDPR, 2016).
A privacy impact assessment (PIA) is a process of assessing the possible privacy implications of new uses of personal data (Write & Hert, 2012). PIA is the process that helps organizations determine their risky actions with respect to the related law. In PIA the effects and risks of processing personal identifier information for the organization is considered. Consecutively how organizations should collect, maintain and process personal data in order to propose some solution for mitigating or terminating these risks is interpreted (HIQA, 2017; ICO, 2015; SEC, 2007). Since PIA provides a holistic approach that considers all dimensions of the privacy, data protection impact assessments (DPIA) were presented to focus on legal-compliance and to process data that is consistent with the GDPR (Binn, 2017). Clarke (2011, 2016) states that 'Data Privacy Impact Assessment is a study of the impacts of a project on only the privacy of personal data; whereas a PIA considers all dimensions of privacy'. Furthermore, a standard for privacy impact assessment was presented as ISO/IEC 29134.

PIA can be critical for GDPR compliance projects for the protection of sensitive personal data but it is not required for TDPL projects in Turkey. TDPA published guidance for technical and managerial controls for information security and it is used in the compliance process instead of PIA.

Health Information and Quality Authority (HIQA) states that "Although a PIA should be more than simply a compliance check, it does nevertheless enable an organization to demonstrate its compliance with the privacy legislation in the context of a complaint, privacy audit or compliance investigation. In the event of an unavoidable privacy risk or breach occurring, the PIA report can provide evidence that the organization acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation" (HIQA, 2017).

PIA consists of two basic risk categories. The first one is a risk to individuals, which is a type of risk resulting from risks such as identity theft. The second one is a risk to institutions, which is a type of risk arising from the lack of compliance to law and data breaches (IPC, 2015; ICO, 2015).

Organizations will have a lot of advantages when they exercise a PIA study covering all of their new projects or departments. The first benefit of the PIA is that organizations will be able to collect, maintain and process huge amount of personal data in accordance with the law. Also, the decision making process is smoothed out in case of an emergency situation because the PIA documents include what needs to be done if a pre-defined risk occurs. Therefore, organizations can make sure that they will apply the best practices against specific risks. In addition to this, employees or people responsible from risk can react to the risk swiftly since employee's awareness increase due to the PIA studies. This is so because the PIA documents explain roles and responsibilities of all departments and individuals in detail. When organizations determine the timeframe for which 'personal data' is needed based on their business purposes and related legislations, they can find the optimal duration. Therefore, they can make monetary benefits and increase their system efficiency by managing their cost, which is based on the duration of the data staying in the database. They can then use this data in a systematic way (IPC, 2015; ICO, 2015).

There are some steps for consulting organizations to obtain the PIA document or report in order to be capable of taking actions against all potential risks that may arise within the company. These steps are preliminary analysis, project analysis, privacy analysis and PIA report (IPC, 2015).

Preliminary Analysis/Review

In this step, consulting firms or other third party firms collect information in order to understand the company. This information includes which sector the company serves, sectoral requirements and organizational standards of the company. Therefore, consultants will be able to formulate a project compliance plan related to personal data protection for the company (IPC, 2015).

In this phase, consulting firms share a file which covers following titles to understand what type of personal information is maintained and how this data is processed within the departments of the organization (Di Iorio et al. 2009;IPC, 2015; ICO, 2015);

- Which department collects personal information?
- What type of personal information is collected from customers (name surname, religion and etc.)? This information can be categorical such as medical records instead of name, surname and disease because if an organization has a lot of departments, it can be hard to collect this data.
- Which method is used while collecting personal data? (oral, documents, other organizations)
- Is there any permission or explicit consent of customers?
- What is the business purpose of using this information (i.e.: giving required service)?
- Is there any retention period of this information?
- Is this information being shared with third countries, parties or even different departments within the company?
- Is private data being transferred abroad.

After this process, if the company collects and processes personal information, consulting firms move to second step which is the project analysis (IPC, 2015; SEC, 2007).

Description of the context PIA

In conducting PIA it is essential to explain the compliance project goals to be realized and benefits for the organization, individuals and to other parties. It can be helpful to refer other related documents, such as a project proposal. Interviews with departments could be useful to understand the business goals. Also this provides a double check for compliance if information is missing or if the company considers that there are some unaddressed parts related to the information. To understand project goals following questions could be useful:

- In which sector does the company serve and what are the business processes?
- Which technology is used within the company?
- Which security measures are taken against privacy risks?
- Are safeguards compatible with the Law?
- What is the risk assessment methodology of the company?
- What are the privacy policies and procedures of the company with third parties?

Description of the Information Flows

The collection, usage and deletion of personal data should be explained in this stage. It may also be convenient to give a flow diagram and explain data flows. For example, the workflow given in Fig. 2 shows organizational structure and processes clearly. If there is missing information about their business process for data processing, these flows provide feedback to the organization. Therefore, they agree on a common ground so consulting firms can go ahead according to these flows.

As an example, In Fig. 2, the data release of the company to its internal departments and to an outside third party is expressed. In Fig. 2, all departments in the company can request a report when they need it in their daily or routine process. If a report is available and there is no need for additional approval related to a data privacy issue, the associated department could access the reports via reporting mechanism. If departments need external assistance while creating the report, the requested report can be generated and delivered to technical experts. Even if the report is not available and there is a need for a report in a different format, technology teams can prepare this report format. If a department demands a report, which is not consistent with the default data, the new report format should be examined by the information security team (IS Team). IS Team can evaluate security need, risk and legal compliance with respect to law and regulations. If IS Team gives approval after their control, the new report template can be available to the related departments. Otherwise, it will be rejected. As a result of this, all authorized departments can access this report, and of course, the personal data of customers and these departments can easily transfer data to third parties.

As a summary, drawing information flows will help show the data life cycle also and make easier personal data management in the company.

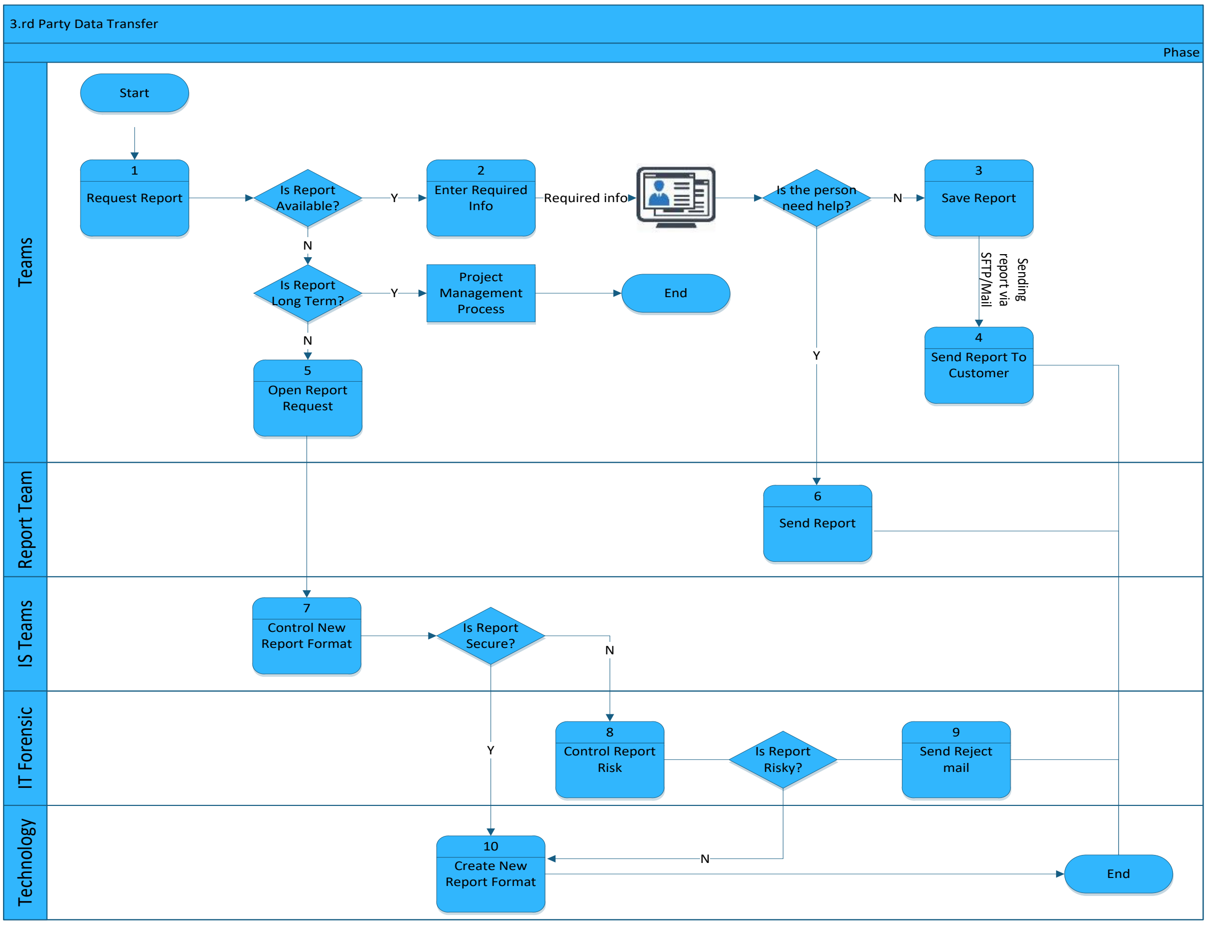


Figure 2. Example information flow: Data Transfer with Third Parties

Risk Assessment

This section uses information gathered from the previous step in order to identify all risks that a company faces and provide appropriate solutions to them in accordance with the Law (ICO, 2015; ISO/IEC 29134). In this step privacy risks that have potential adverse effects on customers are determined. An example is a leakage resulting from unauthorized collection and usage of personal data. Such disclosure of personal data can damage a person financially and have a negative reputational effect on an organization’s prestige. (IPC, 2015).

Therefore, in this step, consulting firms should point out the following items that may cause privacy risks:

- Personal data processing is compatible with legislations.
- There is no usage of outdated personal information
- There is no sharing of personal information with irrelevant third parties and countries
- There is no collection of unnecessary personal information for business processes
- There is no maintenance of personal information longer than the maximum retention period or the optimum duration which the business needs
- The business is taking adequate security measures for protecting personal information (GDPR, 2016;IPC, 2015; POM, 2010)

In this step, consulting firms should also analyze the gap between the law in force and the prevailing situation of the companies related to the compliance process. Also, in this step, it could be useful to benefit from information security frameworks and standards for risk assessment, such as ISO 27001 and ISO 29134. Therefore, using PIA in a TDPL compliance project leads to a more detailed and rich risk assessment. Implementation of ISO 27001 standard in an enterprise could be a GDPR compliance facilitator (Lopes, 2019).

Description of the Risk Response

After the PIA risk document is created, organizations will develop solutions for related risks. The final step for the organization is to decide how to manage specific risks in data inventory. Later, the actions that will be taken to reduce the risks, who the privacy risks that will be involved in the project are approved by and what solutions are required will be discussed.

There are four main responses to risk that top management should consider:

Risk Reduction: Organizations can choose risk mitigation/reduction as a response against the risk. With this approach, organizations try to decrease the possibility of risk occurrence and minimize the impact of the risk on their business processes. Organizations can review their requirements or they can test their novel systems/software before these systems go live in the production environment (CSX, 2015; Hajmohammad & Vachon, 2015).

Risk Avoidance: Organizations try to eliminate a particular risk in order to get rid of the consequences of the risk. Therefore, they make an effort in reducing the probability and impact of the risk to zero by removing the threat. For example, if you live in Istanbul and there is a risk of earthquakes, you can move to another city which has a low likelihood of an earthquake (CSX, 2015; Hajmohammad & Vachon, 2015)

Risk Transfer or Sharing: If the risk level is higher than the tolerance level of the organization and removing the risk source requires a lot of effort and financial resources, the organization can share the responsibility of the risks by making a contractual agreement with insurance companies (CSX, 2015; Hajmohammad & Vachon, 2015).

Risk Acceptance: If the risk is lower than the organizations' tolerance level and the damage that may possibly occur is acceptable in comparison to the effort arising from reducing the risk, then organizations can accept the risk. Although organizations are aware of the risk, they do not take any action toward the particular risk. This approach can be reasonable when the risk likelihood is too low. Nevertheless, when the risk occurs, the organization can take proper action. For example if there is a risk of earthquake within the company environment, the company can decide to stay where they are, considering that moving is more costly (CSX, 2015; Hajmohammad &Vachon, 2015).

Privacy Impact Assessment Report

After the four steps, an organization gets the PIA report. The possible PIA outcomes are integrated back into the project plan. This report provides individuals with a guideline to apply the best solution in a risky environment. Thus, the employees can give more informed decisions as a result of the findings of the PIA steps (IPC, 2015). The document basically covers the type of risks the organization have, the responsible individuals for the risk, the proposed solutions, the sources of risk, the levels of risk, the likelihood of risk and the impact of the risk (HIQA ,2017). This report should be updated when organizations start a new project, establish a new campaign or create a new department (IPC, 2015). In this stage following questions can be useful: “Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?" Or "Who is responsible for implementing the solutions that have been approved?"

CONCLUSION

In order to improve international trade with European countries, Turkish enterprises should also comply with GDPR. In Turkey the associated law is gathered under TDPL. One of the bridges between TDPL and GDPR can be attained using the privacy impact assessment (PIA) report methodology.

The benefits of conducting a PIA are plenty. From individuals perspective, it reassures the individuals that the organizations which use their information have followed best practice. Again from the same perspective, it improves transparency and makes it easier for individuals to understand how and why their information is being used. From the perspective of the organizations, the PIA process will improve how they use information that impacts individual privacy and reduces the likelihood of failing to meet their legal obligations. It will also help an organization build trust with the customers and help understand them. Furthermore, there can be financial benefits of PIA such as identifying a problem early on and amending it with less cost. PIA can also reduce the ongoing costs of a project by minimizing the amount of information being collected or used where this is possible, and devising more straightforward processes for the staff (ICO, 2015).

This study summarizes what the Turkish companies currently do for compliance, and what they can do to comply with GDPR utilizing the PIA report in addition to their TDPL preparations.

REFERENCES

Acquisti, A. (2010). *The Economics of Personal Data and the Economics of Privacy*. Retrieved July 18, 2016, from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1347&context=heinzworks

Biagini, L. (2018, July 20). *Don't Confuse GDPR Compliance with Security*. Retrieved November 4, 2019, from https://www.forbes.com

Billows, D. (2015, September). *Why Projects Fail So Often?*. Retrieved November 4, 2019, from https://4pm.com/2015/09/27/project-failure/.

Binder, D. (2016). *Inside Privacy*. Retrieved December 15th 2019, from https://www.insideprivacy.com/united-states/federal-government-releases-final-guidance-on-cisa/

Binns, R. (2017). Data protection impact assessments: A meta-regulatory approach. *International Data Privacy Law*, 7(1), 22-35.

Burger, R. (2016, September*). 20 Surprising Project Management Statistics*. Retrieved November 4, 2019, from https://blog.capterra.com/surprising-project-management-statistics/.

Burri, M., & Schär, R. (2016). The reform of the EU data protection framework: outlining key changes and assessing their fitness for a data-driven economy. *Journal of Information Policy*, 6(1), 479-511.

Calzolari, G., & Pavan, A. (2006). On the optimality of privacy in sequential contracting. *Journal of Economic theory*, 130(1), 168-204.

Clarke, R. (2011). An Evaluation of Privacy Impact Assessment Guidance Documents, *International Data Privacy Law* 1(2). Retrieved November 4, 2019, from http://www.rogerclarke.com/DV/PIAG-Eval.html

Clarke, R. (2016). *Regulatory Failures in the Security Space: Some Current Cases*. Retrieved November 4, 2019, from From http://www.rogerclarke.com/DV/RFSS.html.

DG Connect. (2018, November 12). *Commission signs agreement with cybersecurity industry to increase measures to address cyber threats*. Retrieved 2019, from https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-cybersecurity-industry-increase-measures-address-cyber-threats.

DG Connect. (2016, July 6). *Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide Taumi Taumi rules on cybersecurity*. Retrieved November 3, 2019, from https://ec.europa.eu/digital-single-market/en/news/statement-vice-president-ansip-and-commissioner-oettinger-welcoming-adoption-first-eu-wide

Di Iorio, C. T., Carinci, F., Azzopardi, J., Baglioni, V., Beck, P., Cunningham, S., ... & Federici, M. O. (2009). Privacy impact assessment in the design of transnational public health information systems: the BIRO project. *Journal of Medical Ethics*, 35(12), 753-761.

Dülger, M.V. (2019). *Kişisel Verilerin Korunması Hukuku*. İstanbul: Hukuk Akademisi Yayıncılık

GDPR (2016), Regulation (EU) 2016/679 (General Data Protection Regulation), Official Journal of EU.

Flaherty, D. (2000). Privacy impact assessments: an essential tool for data protection. *Privacy Law & Policy Reporter*, 5, 85.

HIQA. (2017). Guidance on Privacy Impact Assessment in health and social care, *Health Information and Quality Authority*. Retrieved November 2, 2019, from https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf

ICO (2012, December 12). *What is personal data? – A quick reference guide*. Retrieved November 3, 2019, from https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

ICO (2015). *Conducting privacy impact assessments code of practice*. Retrieved October 2, 2019, from https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

IPC (2015). *Planning-for-Success Privacy Impact Assessment Guide*. Retrieved November 2, 2019, from https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf

ISO/IEC 29134 (2017). *Information technology — Security techniques — Guidelines for privacy impact assessment*. Retrieved November 3, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en.

Kaya, K. (2017). *Kişisel Verilerin Korunması Kanunu Çerçevesinde Veri Tabanı Sistemlerinin Yönetilmesi*. Retrieved November 4, 2019 from http://kdkaya.blogspot.com/2018/03/kisisel-verilerin-korunmas-kanunu.html

Lloyd, I. J. (2017). *Information technology law*. Oxford University Press.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of Information Systems Engineering & Management*, 2(4), 1-8.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and* think. Houghton Mifflin Harcourt.

Monica, N. & Kumar, K. R. (2013). Survey on Big Data by Coordinating MapReduce to Integrate Variety of Data. *International Journal of Science and Research (IJSR)* ISSN (Online), 2319-7064.

Newman, A. (2008). Protectors of privacy: *Regulating personal data in the global economy*. Cornell University Press.

SEC. (2007). *Privacy Impact Assessment (PIA) Guide*. Retrieved November 3, 2019, from https://www.sec.gov/about/privacy/piaguide.pdf

Siegel B. (2016). *What is the difference between privacy and security?*. Retrieved November 4, 2019 from https://www.csoonline.com

TBDL (2016). *The Law on the Protection of Personal Data No. 6698*. Official Gazette of Turkish Republic. enacted on 7 April 2016 and No. 29677

Tuomi, I. (1999). Data is more than knowledge: Implications of the reversed knowledge hierarchy for knowledge management and organizational memory. *Proceedings of the 32nd IEEE International Conference on Systems Sciences*, Hawaii 1999. HICSS-32. pp. 12.

Varkonyi, G. G. (2017). Evaluation on Turkey's Data Protection Adventure. *Eur. Data Prot. L. Rev.*, 3, 238.

Whitney, H. (2012). *Data insights: new ways to visualize and make sense of data*. Newnes.

Wright, D., & De Hert, P. (2012). *Introduction to privacy impact assessment. In Privacy Impact Assessment*. Springer, Dordrecht.

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review*, 28(1), 54-61.

Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, 2017(6), 8-11.