Reflections from GDPR to Turkish Data Protection Act in the Context of Privacy Principles

Ahmet M. Geden[1*], **Türksel Kaya Bensghir**[2]

1 Gazi University, **2** Ankara Hacı Bayram University, * Corresponding author, ahmet.geden@gazi.edu.tr

Abstract

In this paper; we put forward the key changes introduced in the General Data Protection Regulation (GDPR) framework, particularly referring to its underlying privacy (data protection) principles. Besides; we examine the historical roots of the Turkish Law on Protection of Personal Data (KVKK) and its referring set of principles.The study provides a comparative analysis of the privacy principles imposed in both frameworks with their brief explanations and key aspects. Since GDPR is globally regarded as one of the newest and most comprehensive legislation in the field of data protection, we highlight the gaps and probable changes that will affect KVKK based on GDPR. The study reveals that KVKK framework lacks a fundamental principle; "Accountability" for effective implementation of data protection principles.

Keywords: GDPR, Privacy principles, Accountability, Law of Turkish data protection, KVKK.

Citation: Geden, A. M. Bensghir, T. K. (2018, October) *Reflections from GDPR to Turkish Data Protection Act in the Context of Privacy Principles*. Paper presented at the Fifth International Management Information Systems Conference.
Editor: H. Kemal İlter, Ankara Yıldırım Beyazıt University, Turkey
Received: August 19, 2018, **Accepted:** October 18, 2018, **Published:** November 10, 2018

Introduction

Development of Information and Communication Technologies (ICTs) at an unprecedented pace and their widespread use has paved the way for collection, storage, processing and distribution of personal data. Rapid developments and diversification of data processing technologies increased concerns about privacy and individuals' reduced control over their personal data as well. This has led to a constant change in the way the public and private sectors view personal data and has enabled the development of data protection policies.

Since the protection of users' privacy became a remarkable concern, plenty of privacy principles have been established. Among these, OECD's eight privacy principles proposed in 1980 are the most widely referred privacy principles which also inspired many privacy legislations including Directive 95/46/EC (Makri & Lambrinoudakis, 2015, p. 220; OECD Council, 1980).

Greenleaf recognizes Sweden's Data Act (1973) as the first comprehensive data privacy law at the national level. The aim is to implement a set of principles, which are known today as data protection principles in most of the jurisdictions (Greenleaf, 2014, p. 5). Since then, more than 120 countries have enacted privacy laws and a 30 more is on the way. All these jurisdictions bring comprehensive privacy laws for the sake of public/private sectors based on the requirements of international agreements and standards (Greenleaf, 2017, p. 1).

Turkey; quite a long time after, passed its first comprehensive data protection act in 2016. The Law on Protection of Personal Data (KVKK) is fully in force by 7 April 2018. Simultaneously, built on its substantial years of experience and in need of rapid technological developments, EU adopted a new legislation in 2016. The General Data Protection Regulation (GDPR); globally regarded as one of the newest and most comprehensive legislation in the field of data protection, became applicable in May 2018, and replaced its predecessor, Directive (95/46/EC) (EU-FRA, 2018, p. 17; Ministry of Justice, n.d.; Varkonyi, 2017, p. 241).

KVKK was prepared in line with repealed EU Directive 95/46/EC, except for a few points customized. Simply; KVKK may be regarded as a translation of the Directive, which in turn is also a predecessor of GDPR. Bearing this in mind; it would not be difficult to predict which changes would take place in Turkey's personal data protection regime by looking at GDPR (Varkonyi, 2017, p. 238).

Since most privacy laws are structured on a set of data protection (privacy) principles; it would be a rational approach to start with a comparative analysis of underlying principles of two legislations. This would benefit a high-level prediction of probable structural changes that may come up with KVKK. So; this study aims to understand the privacy framework (underlying principles) of two legislations, and based on GDPR, identify and highlight the gaps of KVKK framework.

Historical Background of the Protection of Personal Data in Turkey

Turkey signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) on January 28th, 1981, soon after the Treaty

opened. On the other hand, contrary to Turkey's post-haste signature, it was not until 2016, to ratify the Convention (Council of Europe, 1981).

Apparently; as covered in many studies, for almost 35 years, personal data protection was not explicitly emphasized in the Turkish Constitution as a human right (Doğu, 2017; Henkoğlu, 2017; Küzeci & Boz, 2017; Varkonyi, 2017). It was the Constitutional Reform Referendum in 2010, which added a paragraph in Article 20 of the Constitution mentioning personal data protection.

Although there were incomplete attempts, especially after 2008, to validate a comprehensive data protection law in Turkey, no concrete results were achieved until April 2016 (Varkonyi, 2017, p. 238). Finally, Turkish parliament enacted the Law on Protection of Personal Data (KVKK), and it is published in Official Gazette on April 7th, 2016, including a two year transition period for the Law to be fully implemented (Ministry of Justice, n.d.). Both as an OECD and Council of Europe member Turkey was the last to enact its data protection law (Greenleaf, 2017).

Even though there was a patchwork of personal data protection terminology contained within sector-specific regulations, such as healthcare or commercial sector, none of these were able to provide a comprehensive framework. Thus, KVKK regarded as the first committed privacy and data protection statute in Turkey.

Methodology

Our main research question in this paper was set to be: What are the changes (conceptually and particularly referring to the privacy principles) introduced by GDPR in comparison to KVKK. The purpose here is not to provide an in-depth coverage either for GDPR or KVKK. Instead, the aim is to identify the basic set of principles imposed in two legislations as well as clarify their conceptual meaning and key aspects. With this aim we conduct a comparative analysis of each framework. During comparative analysis; for a specific data protection principle in GDPR, if a direct reciprocal exists in KVKK, we do give the corresponding article number and its text, followed by a brief explanation of the principle. These explanations are mostly referred to the handbooks provided by public or regulatory bodies for both frameworks, where possible. In cases where a direct reciprocal of the principle under consideration is not noticed at first glance in KVKK, we do make a further word-based search (including secondary regulations, handbooks and guidelines etc.) whether an indirect reciprocal exists. In the end, we summarize them in a table form to highlight the missing principles in KVKK framework and probable changes that will affect the Turkish data protection legislation in the future.

GDPR versus KVKK: Privacy Principles

There are basic principles on the processing of personal data which are commonly accepted in international agreements and reflected in legislations of many countries. Both KVKK and GDPR lay on a set of principles which structure the framework of personal data protection regime.

This section gives an overview of the basic set of principles imposed in two legislations and their conceptual meaning. In order to make it easy for the reader, this overview is given in a comparison chart. Table 1; for each of privacy principle headed, gives its corresponding article number and body of the text, following a literal explanation. Since GDPR is the most up to date legislation, privacy principles of GDPR discussed first, while highlighting key points. Moreover, in the third column corresponding KVKK principles with a focus of reciprocity in GDPR are given. (See Table 1)

Findings and Discussions

The GDPR introduces new definitions as in Article 4 compared to KVKK, which are out of the scope of this paper. Regarding information given in previous sections and the comparison in Table 1; one can judge, principles that build up KVKK framework are overlapping with GDPR. Moreover, they both are written flexible enough to comply with the technological developments related to the processing of personal data.

Based on implementation and moving from past experience GDPR attempts to further clarify the existing principles in repealed EU Directive, as well as in KVKK. The main differences and additions in underlying principles of GDPR framework are: accountability (Article 5(2)) and transparency (Article 5(1)(a)) of data processing (Bhaimia, 2018; EU-FRA, 2018; Tikkinen-Piri, Rohunen, & Markkula, 2018).

In addition to the lawful and fair processing of data, GDPR mandates the nature of processing to be transparent relevant to the data subject. Accountability principle; somewhat symbolizes the paradigmatic shift in GDPR. Different from the theoretical nature of other principles in Article 5 (1), accountability put flesh on the bones of all other principles by promoting compliance. It refers to the controller's responsibility in demonstrating compliance with GDPR provisions. With its inclusive nature, the rules strictly linked to it, various new ways of measures and governance activities to facilitate compliance; makes this principle more practical than remain in theory.

We cannot see direct equivalents of these two principles under KVKK, although there appears to be a close interpretation for transparency implied in some of the handbooks published by Personal Data Protection Authority (PDPA) (Kişisel Verileri Koruma Kurumu, n.d., p. 2; Ministry of Justice, n.d.).

Accountability is the keystone of the regulatory framework of GDPR and considered as the primary factor for effective implementation of data protection principles (Cerasaro, 2017). To do that GDPR brings about many new concepts and various ways of governance activities linked to the accountability principle to facilitate compliance:

- As in Article 30, there is an obligation for recording processing activities and making these records available to the regulatory body upon request.
- In certain circumstances, where main activities of the organizations (including public authorities) consist of processing of large scale of personal data via regular and systematic monitoring of data subjects, designating a Data Protection Officer (DPO) may be mandatory. DPO's role here is to monitor compliance with GDPR and the privacy policies, as well as inform and advise the organizations in issues relating to personal data protection (Article 37-39).
- If the type of the processing is likely to result in high risks to the rights of individuals, organizations are obliged to direct a Data Protection Impact Assessment (DPIA) (Article 35).
- Establishing a data protection by design and by default mentality in processes would mitigate most of the risks before they occur (Article 25).

- Implementation of procedures and modalities for the exercise of the rights of the data subjects (Articles 12 and 24).
- Moreover, adherence to certification mechanisms, seals and marks or codes of conduct would also promote compliance (Articles 40 and 42) (Bhaimia, 2018, p. 25; EU-FRA, 2018, p. 134; The European Parliament and The Council of The European Union, 2016).

Accountability principle added to the framework of GDPR after long-standing discussions and based on the advice of the Article 29 Working Party (WP29) of EU. Leading motive was the need of additional tools for ensuring the effectiveness of privacy laws in practice. Moreover, accountability is a material consequence of the concept of trust (Cerasaro, 2017).

Conclusions

It looks like that KVVK framework lacks the accountability principle and its relevant new concepts (such as Data Protection by Design and by Default, DPIA, assigning a DPO, certification mechanisms, seals and marks or codes of conduct, the clearer guidelines on receiving data subjects' consent) which has already promoted in GDPR.

In conclusion; if Turkey wants to step up forward with effective implementation of KVKK, a careful analysis of these new concepts in GDPR should be carried out and taken into account by legislature (Helvacioglu & Stakheyeva, 2017, p. 814). Maintaining a higher level of harmonization with data protection standards and international agreements could be achieved at the very first stage by embedding accountability principle, (as a key driver for effective implementation of data protection principles (Cerasaro, 2017, p. 225)), and its practical implications into Turkey's data protection framework.

This will also help on clarifying legal uncertainties and building a trustworthy relationship between data controllers, individuals, processors and other partners as well, which was also a primary objective during the adoption of GDPR (Cerasaro, 2017, p. 215).

References

Akıncı, A. N. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi. Ankara.

Bhaimia, S. (2018). The General Data Protection Regulation: the Next Generation of EU Data Protection. Legal Information Management, 18(01), 21–28. https://doi.org/10.1017/S1472669618000051

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. International Data Privacy Law, 6(2), 77–78. https://doi.org/10.1093/idpl/ipw006

Cerasaro, E. F. (2017). Accountability principle under the GDPR: is data protection law moving from theory to practice? Retrieved August 7, 2018, from http://lawreview.luiss.it/files/2016/09/Accountability-principle-under-the-GDPR-Is-data-protection-law-moving-from-theory-to-practice.pdf

Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Retrieved July 5, 2018, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/

Doğu, A. H. (2017). Kişisel Verilerin Korunmasına Genel Bir Bakış. Retrieved June 21, 2018, from http://ceur-ws.org/Vol-2045/34_Bilisim_2017_paper_23.pdf

EU-FRA. (2018). Handbook on European Data Protection Law (2018th ed.). Luxembourg: European Union Agency for Fundamental Rights and Council of Europe. https://doi.org/10.2811/343461

Greenleaf, G. (2014). Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. Journal of Law, Information and Science, 23(1), 4–47.

Greenleaf, G. (2017). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. Privacy Laws & Business International Report (Vol. 45).

Helvacioglu, A. D., & Stakheyeva, H. (2017). The tale of two data protection regimes: The analysis of the recent law reform in Turkey in the light of EU novelties. Computer Law & Security Review, 33(6), 811–824. https://doi.org/10.1016/J.CLSR.2017.05.014

Henkoğlu, T. (2017). Veri Koruma Kanununun Getirdikleri. Journal of Current Researches on Social Sciences (JoCReSS). https://doi.org/10.26579/jocress-7.2.18

Kişisel Verileri Koruma Kurumu. (n.d.). Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler. Retrieved July 19, 2018, from https://kvkk.gov.tr/SharedFolderServer/CMSFiles/d0fbca08-30af-41fe-a7c9-65663b9c5231.pdf

Küzeci, E., & Boz, B. (2017). The new Data Protection Act in Turkey and its potential implication for E-commerce. International Data Privacy Law, 7(3), 219–230. https://doi.org/10.1093/idpl/ipx007

Makri, E.-L., & Lambrinoudakis, C. (2015). Privacy Principles: Towards a Common Privacy Audit Methodology. In S. Fischer-Hübner, C. Lambrinoudakis, & J. López (Eds.), Trust, Privacy and Security in Digital Business: 12th International Conference, TrustBus 2015, Valencia, Spain, September 1-2, 2015, Proceedings (pp. 219–234). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-22906-5_17

Ministry of Justice. (n.d.). Law on Protection of Personal Data. Retrieved June 20, 2018, from http://www.judiciaryofturkey.gov.tr/English-version-of-Law-on-Protection-of-Personal-Data-is-available-on-our-website

OECD Council. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved October 16, 2016, from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

The European Parliament and The Council of The European Union. General Data Protection Regulation, Pub. L. No. Regulation (EU) 2016/679, Official Journal of the European Union 88 (2016).

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Varkonyi, G. G. (2017). Evaluation on Turkey's Data Protection Adventure. European Data Protection Law Review (EDPL), 1, 238–243.

Table 1. A Comparison of referred Data Protection (Privacy) Principles of GDPR and KVKK.

Principle	General Data Protection Regulation (GDPR)	Turkish Law on Protection of Personal Data (KVKK)
(1)-lawfulness, fairness and transparency	**Article 5-(1)(b)** *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;* Personal data processing should stick on the core principles of lawfulness, fairness and transparency. To process lawfully mean(s) having a lawful base and not being against other laws. Article 6(1) defines these lawful grounds. Fair processing actually governs the relationship between the controller and the data subject and requires informing the data subject about potential risks of processing and ensuring that there will not have unforeseen adverse effects. In other words, it is about processing the personal data in an ethical way, beyond the obligations of transparency principle. Lastly, transparency is about informing the data subjects before processing their data with all relevant details including the purpose, risks and safeguards of processing or their rights. This information (mostly known as privacy notices) should be clear and plain so that it makes it easier for the data subject to understand his/her rights (Bhaimia, 2018, p. 25; EU-FRA, 2018, p. 117)	**Article 4-(2)(a)** *Being in conformity with the law and the principle of bona fide,* Conformity with the law (lawfulness) and honesty implies the obligation to act in accordance with the principles of law and other legal arrangements while processing personal data. This principle has an inclusive nature. In general, it means being in compliance with legal norms and universal law principles. Lawfulness has a broader scope, also includes legislative compliance. What is implied by conformity with the rules of honesty is not violate the honesty rule defined in Article 2 of Turkish Civil Code while processing personal data and requires being in respect to the abuse of the right (Kişisel Verileri Koruma Kurumu, n.d., p. 2).
(2)- purpose limitation	**Article 5-(1)(b)** *Personal data be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;* Purpose limitation requires defining a specific purpose of processing before starting. Once a well-defined original purpose is set, no further or secondary processing, incompatible with the initial one is allowed. In Article 6(4); GDPR brings some factors for the compatibility check of the secondary purpose and lays down rules in case of a secondary purpose of processing other than for which the personal data has been collected (Bhaimia, 2018, p. 25; EU-FRA, 2018, p. 122).	**Article 4-(2)(c)** *Being processed for specified, explicit and legitimate purposes,* In essence, the context has a similar meaning with GDPR. The principle aims to; • Ensure that personal data processing activities are clearly understandable by the data subject, • Determine the legal background of the data processing activity, • Ensure personal data processing activities and its purpose specificity is set forth in detail (Kişisel Verileri Koruma Kurumu, n.d., p. 7).
(3)- data minimization	**Article 5-(1)(c)** *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;* Data minimization is all about strictly limiting the collection of data and categories of data chosen to the specified purpose of processing. Collected information should be directly relevant with and should not go beyond the amount as necessitated by the well-defined purpose of processing (Bhaimia, 2018, p. 25; EU-FRA, 2018, p. 125).	**Article 4-(2)(ç)** *Being relevant, limited and proportionate in relation to the purposes for which they are processed,* The article has a very similar statement with GDPR, except the term "adequate". It refers to the fact that the processed data should be convenient for performing the specified purposes of processing. And, processing of personal data that is not relevant or necessary must be avoided. In addition, the processed data should be limited to the one required just for performing the specified purpose. The principle of proportionality means establishing a reasonable balance between the data processing and the intended purpose (Akıncı, 2017, p. 32; Kişisel Verileri Koruma Kurumu, n.d., p. 9).

Table 1 (cont). A Comparison of referred Data Protection (Privacy) Principles of GDPR and KVKK.

Principle	General Data Protection Regulation (GDPR)	Turkish Law on Protection of Personal Data (KVKK)
(4)- accuracy	**Article 5-(1)(d)** *Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;* The principle of accuracy should be implemented by the data controller, which means data controller is responsible to take every reasonable step in all data processing operations. Ensuring accuracy is about erasing or rectifying inaccurate data with no delay and may require a regular checking of data and keeping it up to date (where necessary) (EU-FRA, 2018, p. 127).	**Article 4-(2)(b)** *Being accurate and, when necessary, up-to-date,* In essence, the statement is very similar and the context has a similar meaning with GDPR. Accuracy of the personal data processed by the controller is very important both for the data subject and for the processor and this principle give responsibility to the controller. Maintaining the data up-to-date requires acting together with the data owner. This is also in line with the right of data subjects to request correction of their data (Akıncı, 2017, p. 32; Kişisel Verileri Koruma Kurumu, n.d., p. 5).
(5)- storage limitation	**Article 5-(1)(e)** *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;* Storage limitation principle requires deletion or anonymization of the personal data at the shortest notice, if it is no longer needed for the purpose of gathering (EU-FRA, 2018, p. 129).	**Article 4-(2)(d)** *Being stored for no longer than is provided in the relevant legislation and is necessary for the purposes for which data are processed.* In accordance with the purpose limitation principle, there are retention periods set by the data controller for storage of personal data, as well as these periods may be determined under relevant legislation to which the data controller is obliged to. Accordingly; if there exists a period projected for data controllers and/or relevant personal data, this period should be respected. Otherwise the data must be kept only for the time required for the purpose which the data being collected. If there is no valid reason for further storage of data, that data must be deleted or anonymized. Personal data should not be kept for with the thought that it may be needed again in the future or for any other reason (Kişisel Verileri Koruma Kurumu, n.d., p. 11).
(6)- integrity and confidentiality (data security)	**Article 5-(1)(f)** *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;* Data security principle requires implementation of appropriate security measures whether they are technical or organizational in nature. Main purpose is to protect data against unlawful, unauthorized or accidental actions (access, use, modification, loss, damage or disclosure etc.). This principle is also linked to mandatory data breach notification detailed in Article 34. As stated, within 72 hours of becoming aware of a breach, a controller must notify the regulatory authority and/or individuals based on the likelihood of the risks to the rights of individuals. GDPR also introduces pseudonymization as a process that can protect personal data and mitigate the risks in case of a breach. Regular reviews and case by case basis should be the approach to determine whether security measures are appropriate or not (Bhaimia, 2018, p. 25; EU-FRA, 2018, p. 131).	**N/A (No direct equivalent)** Although there is no direct equivalent of the "data security" principle under Article 4, Article 12 defines the obligations regarding data security.

Table 1 (cont). A Comparison of referred Data Protection (Privacy) Principles of GDPR and KVKK.

Principle	General Data Protection Regulation (GDPR)	Turkish Law on Protection of Personal Data (KVKK)
(7)-accountability	**Article 5 - (2)** *The controller shall be responsible for, and be able to demonstrate compliance with above principles;* Accountability is a new principle in GDPR compared to the repealed EU directive. Its inclusive nature over all other principles presumably makes it the most significant one. Inherently, controllers and processors are expected to be accountable although Article 5(2) only targets controllers. They are jointly responsible for maintaining compliance of their operations with GDPR and respective rules which are strictly linked to accountability. The principle of accountability requires implementation of appropriate measures to promote and safeguard data in an active and continuous manner. At any time controllers must be able to demonstrate compliance with legal provisions and the evidence of data protection principles to general public, data subject and regulatory authority. Demonstration of compliance with data protection principles must be done by internal governance and putting in place appropriate controls in a balanced way based on the type of the processing and the risks that they may come up (Bhaimia, 2018, p. 25; EU-FRA, 2018, p. 134).	**N/A (No direct equivalent)** We do make a word based search on KVKK (including secondary regulations, handbooks and guidelines etc.) whether "accountability" principle has any correspondence in Turkish personal data protection legislation. In conclusion and to the very best of our knowledge there is no valuable consideration correspondent to the accountability principle in GDPR either conceptually or textually.