Annales de la Faculté de Droit d'Istanbul, 70: 195–241

DOI: 10.26650/annales.2021.70.0007
http://annales.istanbul.edu.tr/

Annales de la Faculté de Droit d'Istanbul

Submitted: 07.04.2021
Revision Requested: 31.05.2021
Last Revision Received: 27.08.2021
Accepted: 27.08.2021

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law

Kendini İhbar Etme veya Delilleri Yok Etme İkilemi: Kişisel Verilerin Korunması Hukuku Bağlamında Veri İhlal Bildirimi Kurallarının Hukuki Analizi

Mehmet Bedii Kaya*

Abstract

Technology has penetrated every aspect of life and brought security and privacy issues to the forefront of the regulatory landscape. In such a hyper-connected world, security breaches are inevitable. Hence, general legislation in the field of protection of personal data is becoming ubiquitous. The rules are likewise being drafted to ensure the highest degree of privacy and security.

The violation of security requirements can have an unprecedented and catastrophic consequence on data controllers. A security incident can compel the data controller to notify a competent data protection authority of a breach and communicate all facts to affected data subjects. Data breach notification is self-disclosure of the data controller about a personal data-related incident regardless of the intentional or negligent character of the event. The underlying aim of this obligation is to prevent or mitigate all adverse effects or damage deriving from a data breach incident.

This article maps out the legal framework governing data breach notification under the European Union's law, in particular General Data Protection Regulation and the Turkish Data Protection Law. This article maintains that strict and burdensome data breach notification rules do not serve the interest of data protection of individuals as data controllers could refrain from notification and bury the pieces of evidence. Such a notification-phobia is a major threat to the overall cybersecurity realm. The article emphasizes that there is a need for balanced rules and adequate accountability tools which would encourage data controllers to report any data breach incidents without hesitation.

Keywords

Breach, Notification, Data Protection, Privacy, Cybersecurity

Öz

Teknoloji hayatın her alanına girmiş ve güvenlik ile mahremiyeti en temel regülasyon konusu haline getirmiştir. Her şeyin birbiriyle bu denli bağlantılı olduğu bir dünyada güvenlik ihlalleri kaçınılmazdır. Bunun bir neticesi olarak da kişisel verilerin korunması alanındaki düzenlemeler yaygınlaşmaktadır. Nihayetinde amaç en üst düzeyde mahremiyet ve güvenliği sağlamaktır.

Güvenlik yükümlülüklerinin ihlali veri sorumluları nezdinde benzeri görülmemiş ve yıkıcı sonuçlar doğurmaktadır. Bir güvenlik ihlali veri sorumlusunu, yetkili veri koruma otoritesine ihlali bildirmek ve aynı zamanda ihlalden etkilenen ilgili kişilere olayın detaylarıyla ilgili haber vermek zorunda bırakmaktadır. Veri ihlal bildirimi, veri sorumlusunun kasten veya ihmali olarak gerçekleşmiş kişisel verileri ilgilendiren bir olaya ilişkin kendisini ihbar etmesidir. Bu yükümlülüğün altında yatan temel amaç, bir veri ihlal olayından kaynaklanan tüm olumsuz etkileri veya zararı önlemek veya azaltmaktır.

Bu makalenin amacı Avrupa Birliği'nin veri ihlal bildirimlerine ilişkin temel düzenlemelerini, bilhassa da Genel Veri Koruma

* **Corresponding Author:** Mehmet Bedii Kaya, (Asst. Prof.), Istanbul Bilgi University, Faculty of Law, IT Law Department, Istanbul, Turkey.
E-mail: mehmet@mbkaya.com ORCID: 0000-0001-5256-9854

To cite this article: Kaya, MB, "Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law", (2021) 70 Annales de la Faculté de Droit d'Istanbul 195. https://doi.org/10.26650/annales.2021.70.0007

Tüzüğünü ve aynı zamanda Türk Kişisel Verilerin Korunması Kanununu incelemektir. Bu makalede katı ve külfetli veri ihlal bildirimi kurallarının veri sorumlularını bildirim yapmaktan imtina edip delilleri yok etmeye ittiği; bu sebeple de bu tür katı düzenlemelerin kişisel verilerinin korunmasına aslında hizmet etmediği tartışılmaktadır. Veri ihlal bildirimi yapma çekincesi genel anlamda siber güvenliğe yönelik önemli bir tehdittir. Bu makale kapsamında veri sorumlularının herhangi bir veri ihlal olayını tereddüt etmeden bildirmesini teşvik edecek dengeli düzenlemelere ve uygun hesap verebilirlik araçlarına ihtiyaç olduğu vurgulanmaktadır.

Anahtar Kelimeler
İhlal, Bildirim, Veri Koruma, Mahremiyet, Siber Güvenlik

Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Breach Notification Rules under the Turkish Data Protection Law

Introduction

Information and communication technologies have evolved into vital instruments for society, politics, and economy. While digitalisation has contributed to the well-being of societies, it has also created new challenges and risks. In such a hyper-connected world, security breaches are inevitable. The need to safeguard privacy by utilizing state-of-art techniques, in this respect, stands at the epicentre of the digitalisation process.

In today's data economy, privacy has developed into a pivotal matter of regulation. General legislation in the field of protection of personal data is becoming increasingly ubiquitous.[1] The rules are also being tightened up to ensure the highest level of privacy and security.

Data protection regulations change how data controllers handle, process, transfer, and retain personal data. The most prominent legal obligation of a data controller, in this regard, is the maintenance of data security. Data breaches are considered one of the most significant threats to organizations.[2] The total average global cost of data breaches is estimated 3.86 million USD.[3] Therefore, violation of security obligations is heavily sanctioned.

The infringement of security requirements can have an unprecedented and catastrophic consequence on a data controller. A breach could turn all the spotlights on a data controller, and a minor incident could destroy the hard-earned reputation of the data controller, which has been built up over the years. Such a violation could trigger a set of civil and criminal lawsuits along with indemnity claims, class actions, and statutory or contractual claims against data controllers and all other stakeholders connected to such an incident.

1 For the data protection legislations around the world see CNIL, '*Data protection around the world*' https://www.cnil.fr/en/data-protection-around-the-world [accessed 1 March 2021].

2 Paul B Lambert, *Understanding the New European Data Protection Rules* (CRC Press - Taylor & Francis 2018) 312.

3 IBM, '*Cost of a Data Breach Report 2020*' https://www.ibm.com/security/digital-assets/cost-data-breach-report/ [accessed 1 March 2021].

The day when a data security breach occurs triggers the doomsday protocols of the data controller; the day when all the compliance projects are tested in a real-life scenario. Due to devastating consequences the data controller faces, the decision to run the alarm bells, i.e., notifying the data breach to the relevant stakeholders, is the most vital and challenging decision to be taken by a data controller as it creates a domino effect of kind.

The data controller, under the pressure of contractual obligations, afraid of losing business and under significant scrutiny of the supervisory authorities could have two simple options: either self-disclosure and bear the consequences or bury the evidence and pray that no one notices the incident. However, such notification-phobia is a major threat to the overall cybersecurity realm.

Contemplating the possible risks arising from non-disclosure, the EU's General Data Protection Regulation (hereinafter GDPR) of 2016, which entered into force on 25 May 2018, introduced a new obligation: data breach notification.[4] The GDPR has defined what constitutes a data breach, when and how to notify those affected and effected by such a breach, what information the notification of breach should encapsulate, the format and procedures of the notification, and exemptions of such obligation.

The data breach notification requirement is likewise a popular issue of Turkey's law and practice. The Turkish Data Protection Law no. 6698 (hereinafter the DP Law) has introduced a general data breach requirement that applies to all data controllers regardless of their sector, size, or the type of data they are processing. However, the rules governing breach notification remain quite complex and controversial because of the ambiguities and disparities concerning the scope, exceptions, substance, and thresholds of notifications. In particular, there is controversy in practice when the breach incident also triggers a parallel criminal investigation. There are also disagreements in determining the timeframe limit for notification as well as the announcement of such breaches to the public.

The primary purpose of this article is to review rules governing the personal data breach notification requirement under the Turkish data protection law. The article addresses what constitutes a breach, when a breach requires notification, what the threshold for notification is, what the procedures of the notification are as well as the exemptions of such requirements (if any), the subsidiarity of having such a general obligation of disclosure, and the prospective consequences of late or inaccurate notification. The article identifies any problem in the legal and institutional framework and attempts to map out any barrier to the efficient functioning of the

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016.

breach notification mechanism. The article, in this regard, lays down possible options for the alignment of Turkish law with the EU acquis.

The overall structure of the article takes the form of five sections. The first section provides an overview of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, aka Convention no. 108. The second section gives an overview of data breach notifications under European Union Law. The third section introduces General Data Protection Regulation (GDPR)'s articulation of data breach notifications and procedural obligations for data controllers and processors.

The fourth section focuses on Turkey's data protection law. This section maps out the regulatory and institutional framework of Turkey on data protection and cybersecurity. The fifth section describes potential reforms that Turkey needs to make based on the EU's experience.

The article examines the topic from a legal perspective and the technical aspects of data security are examined to a certain extent and depth. It is important to note that while the data breach notification is an issue, which is widely regulated under various jurisdictions in different parts of the world, e.g., Australia, Brazil, Canada, Colombia, the Philippines, South Korea, South Africa, Taiwan, Vietnam and the USA,[5] this article will only focus on the EU law. The impetus of this choice derives from the political and legal relevance of the EU to Turkey and most importantly, from Turkey's explicit political target of adopting the EU's data protection norms.

I. The Data Breach Notification Rules Under the Council of Europe's Data Protection Conventions

The first international agreement on data protection, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, or so-called Convention no. 108, is currently ratified by fifty-five states from different regions of the world.[6] The Convention no. 108 is commonly recognised as a foundation instrument of international data protection law.

The Convention no. 108 lays down a crucial rule for data security. According to Article 7 of the Convention no. 108, appropriate security measures must be taken to

5 The USA does not have a federal data protection law. However, there are various federal laws or rules that mandate notification of data breaches such as Financial Industry Regulatory Authority (FINRA), Gramm-Leach-Bliley Act (GLBA), HIPAA-HITECH Act Final Breach Notification Rule, Office of Management and Budget (OMB), Regulation Financial Disclosure (FD), Regulation S-K, Securities Act of 1933, Securities Exchange Act of 1934. For a list of such legislation see NCSL, '*Security Breach Notification Laws*' https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [Accessed 1 March 2021]; see also Mark Burdon, Bill Lane, Paul Von Nessen, '*Data breach notification law in the EU and Australia e Where to now?*' (2012) 28 Computer Law & Security Review 296, 297 et seq; Software vendors would have to disclose breaches to U.S. government users under new order: draft https://reut.rs/39fy5Xm [Accessed 26 March 2021].

6 Council of Europe, '*Chart of signatures and ratifications of Treaty 108*' https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures [accessed 1 March 2021].

protect personal data stored in automated data files against accidental or unauthorised destruction or accidental loss and unauthorised access alteration or dissemination. The Convention no. 108, though, does not prescribe an additional provision dealing with breach notification.

It could be argued that the lack of an obligation to declare data breaches is a major shortcoming of the Convention. However, considering when this convention was adopted, i.e., the 1980s, the need for data breach notification had not emerged in the international realm as a fundamental safeguard of privacy. Furthermore, considering the level of connectivity, mobility, and overall cyber threats to personal data at that time, the Convention no. 108 cannot be condemned for the lack of an explicit provision to address breach notification.

The revised and updated version of the Convention no. 108, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data or colloquially called the Convention 108+, likewise has attracted tremendous attention in the world. By January 2021, thirty-three states from different regions of the world had committed to transform the legal requirements of this Convention into their national law and eleven states have already ratified this Convention.[7]

The Convention 108+ reinforces the international privacy law through additional safeguards regarding the proportionality and data minimisation principles and lawfulness of the processing; introduction of new data types, e.g. sensitive data, which will now include genetic and biometric data, trade union membership and ethnic origin; higher transparency of data processing; new rights for the new contexts of data processing, e.g. in case of algorithmic decision-making context which is significant in the era of artificial intelligence; greater accountability of data controllers; stipulation of the "privacy by design" principle; implementation of the data protection principles to all processing activities; coherent rules for trans-border data flows; enhanced powers and independence of the data protection authorities, and strengthening legal basis for international cooperation.[8]

The most important innovation of the Convention 108+ inter alia is the obligation to disclose data breaches and the requirement to notify, without delay, any security breaches to the competent authorities. According to Article 7, Section 2, the Signatory States are required to oblige data controllers by law to notify, without delay, at least the competent supervisory authority, of those data breaches which may seriously interfere with the rights and fundamental freedom of data subjects.

7 Council of Europe, '*Chart of signatures and ratifications of Treaty 223*' https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures [accessed 1 March 2021]; Turkey is not party to the Convention 108+.

8 It would be beyond the scope of this article to outline the novelties of The Convention 108+. For such an analysis see Paul De Hert and Vagelis Papakonstantinou, '*The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*' (2014) 30 Computer Law & Security Review 633; see also Council of Europe, '*Council of Europe treaty bolstering data protection opened for signature*' https://go.coe.int/AVgeo [accessed 1 March 2021].

The Convention 108+ sets the minimum criteria for the notification of data breaches. This requirement is limited to cases that may seriously interfere with the rights and fundamental freedoms of data subjects, which should be notified, at least, to the supervisory authorities.[9] The Signatory States have, nevertheless, a wider margin of discretion on this requirement and are entitled to mandate the controllers to notify the data subjects beyond just the competent authorities.

Explanatory Note to the Convention 108+ highlights that the notification made by the controller to the supervisory authorities does not preclude other complementary notifications.[10] Given the fact that a data breach is likely to give rise to physical, material, or non-material damage to data subjects, data controllers should show due diligence and should notify the data subjects to mitigate the adverse effects of the breach.

The recognition of the data breach notification requirement as a fundamental instrument to uphold the rights and freedoms of individuals is a breakthrough in the international data protection realm. It is expected to increase global awareness for data security, as the reporting of such incidents will be statutory in the jurisdictions in the scope of the Convention 108+.

The developments at the Convention 108 are closely monitored by the EU. Recital 105 of the GDPR mandates the European Commission to take account of obligations arising from the third country's participation in multilateral or regional systems in particular about the protection of personal data as well as the implementation of such obligations. The European Commission especially oversees third country's accession to the Convention 108 while assessing the level of protection in third countries or international organisations.

The EU also gives significant attention to the ratification of the Convention 108+. The European Council, on 9 April 2019, has adopted a decision authorising EU member States to "*ratify, in the interest of the Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) insofar as its provisions fall within the exclusive competence of the Union*."[11]

9 Council of Europe, '*The modernized Convention 108: novelties in a nutshell*' https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8 [accessed 1 March 2021].

10 Council of Europe, '*Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*' https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [accessed 1 March 2021].

11 Council Decision (EU) 2019/682 of 9 April 2019 authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data OJ L 115/7, 02.05.2019.

II. The Breach Notification Regulations Under the EU Law

Data security obligation is not an innovation of the GDPR as the Directive 95/46/EC has previously articulated a specific rule for the security of data processing. It is remarkable that Article 17 of Directive 95/46/EC requires that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The provision also highlights that protection measures must ensure a level of security appropriate for the risks represented by the nature of the data to be protected. However, no specific provision laid down rules regarding the notification of data breach under Directive 95/46/EC. This obligation has evolved under different instruments of the EU law and has ultimately become a fundamental pillar of the data protection eco-system after the ratification of the GDPR.

The Directive 2002/58/EC,[12] also known as E-Privacy Directive, which applies to the electronic communication services, requires electronic communication service providers to take appropriate measures to safeguard the security of their services, if necessary, in conjunction with the provider of the network, and to inform subscribers of any special risks of a breach of the security of the network.[13] Due to the importance of sustaining security in the electronic communication sector, Regulation (EU) 611/2013 also laid down guidance to conform to these obligations.[14]

The new information security management approach elaborated by E-Privacy Directive has influenced the Regulation No 910/2014,[15] also known as eIDAS Regulation which was issued on 23 July 2014 and entered into force on 1 July 2016 (except for certain provisions). The eIDAS Regulation has underlined that notification of security breaches and security risk assessments are essential while providing adequate information to concerned parties in the event of a breach of security or loss of integrity.[16]

12 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002.

13 For a comprehensive review of the E-Privacy Directive, in particular, the problems such as conceptual incoherence, limited practical coverage, and compatibility with information privacy law see Burdon, Lane and Von Nessen (n 5). The E-Privacy Directive is currently being reformed and the breach notification rules are also at the forefront of the reform negotiations. See Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (Cambridge University Press 2010), 193.

14 Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173/2, 26.06.2013.

15 Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257/73, 28.8.2014.

16 eIDAS Regulation Recital 38.

Under Article 19(2) of the eIDAS Regulation entitled 'Security Breach', qualified and non-qualified trust service providers are required, without undue delay, in any event within 24 hours after having become aware of security incidents, to notify the supervisory body and where applicable, other relevant bodies such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Notably, in addition to notifying the relevant competent bodies, where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider is also required to notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Another notification obligation is regulated under the Directive 2016/1148,[17] also known as the NIS Directive. This directive, which provides legal measures to boost the overall level of cybersecurity in the EU, entered into force in August 2016.

According to Article 14 of the NIS Directive, essential services operators and Article 16 digital service providers as defined under the NIS Directive are required to notify relevant computer security incident response teams, Computer Security Incident Response Team, also known as CSIRT, of any security incidents having a significant impact on the continuity of the essential services they provide. Furthermore, entities that have not been classified as operators of essential services and are not digital service providers, e.g., information society service providers, may voluntarily notify their users about incidents having a substantial impact on the continuity of the services which they provide as per Article 20 of the NIS Directive.

Payment services are also subject to specific security and notification rules. The Payment Services Directive (hereinafter PSD2),[18] lays down rules for operational and security incidents affecting electronic payments provided by payment services providers. According to Article 95 of the PSD2, the payment service providers are required to establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services they provide.

In addition, as part of that framework, payment service providers need to establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents. Similarly,

17 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, L 194/1, 19.07.2016.

18 Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015.

payment service providers must have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials as per Article 97 of the PSD2.

The PSD2 not only requires notification to the competent authority but in certain cases also requires notification to payment service users. According to Article 96 of the PSD2, in the case of a major operational or security incident, payment service providers are required without undue delay to notify the competent authority in the home member state of the payment service provider.[19] In addition to the notification to the competent authority, the PSD2 also requires notification to the payment service users in certain cases.

Article 96(1) of the PSD 2 stipulates that where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider is required to, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

It is significant to note that data security is often used as equal to cybersecurity. However, cybersecurity is a broader concept and encompasses not merely data, but all information systems as a whole, including but not limited to hardware, software, peripherals, network, and related infrastructure.[20] The primary objective of cybersecurity is to protect assets such as hardware (e.g. computers and smartphones), software, and data.[21] On the other hand, the main objective of data protection regulations is to protect the fundamental rights and privacy of the relevant data subject. It is noteworthy that the data protection regulations are human-centric instruments of law whereas cybersecurity regulations are asset-centric.

Cybersecurity and data protection regulations frequently intertwine. The line between these kinds of regulations is becoming blurred which is evident in the scattering of regulations and directives in multiple statutes and policies. These rules have established the normative background for cybersecurity and information security throughout the EU. Although the fragmentation of the regulatory framework is criticised, having such distinct obligations of notification adds another layer to

19 The rules with regard to classification of major incidents, the content, the format, including standard notification templates, the procedures for notifying such incidents, the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities is determined by the European Banking Agency in accordance with the powers conferred under Article 96 of the PSD2. See, European Banking Authority, '*Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) EBA/GL/2017/10, 27.07.2017*' https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2 [accessed 1 March 2021].

20 Dominik, Herrmann and Henning Pridöhl, '*Basic Concepts and Models of Cybersecurity*' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity* (Springer 2020), 12.

21 *Ibid*. 12.

information security management governance.[22] Furthermore, they contribute to the development of unique incident response mechanisms tailored up for meeting the regulatory framework.

III. The Examination of the GDPR

The GDPR has introduced extensive rules on data security and breach notification. The legislation lays down a general data security obligation, outlines the possible risks and dangers arising from data breaches, puts forth the procedure for notification of a personal data breach to the supervisory authority, and data subjects. It further clarifies the way of communication as well as exceptions and how to justify exceptions.

The GDPR highlights that certain obligations of data controllers including the communication of a personal data breach to a data subject could be restricted as far as necessary and proportionate in a democratic society to safeguard certain public and private interests.[23] In this regard, it should be noted that there might be certain national differences in terms of data breach notification conditions and procedures.

A. What Constitutes a Data Breach?

The GDPR mandates that both controllers and processors have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed.[24] The data security requirement makes a particular structural change that compels the entities to change their business practices, including their procurement practices, vendor relationships, and internal and external audit tools. This obligation requires data controllers to oversee all contractual relations, and mandates specific and strict contractual provisions while entering into any contract involving personal data. As well, it mandates sustainable and effective monitoring of personal data within and throughout the organization.

The GPDR articulates specific security measures that are deemed appropriate.[25] For instance, the pseudonymization and encryption of personal data is a vital security measure. Another fundamental measure is the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. Similarly, the ability to restore the availability and access to personal data promptly in the event of a physical or technical incident and a process for routinely

22 It is argued that the current regulatory framework seems to be offering solutions to the symptoms, rather than the causes. Accordingly, it is suggested that "*[p]art of the problem could be addressed by collecting data on breaches that are mindful of the technological environment, but also by an active attempt to create more harmony among the regulatory patchwork.*" Maria Grazia Porcedda, '*Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*' (2018) 34 Computer Law & Security Review 1077, 21.

23 GDPR Recital 73 and Article 23.

24 GDPR Article 32.

25 GDPR Article 32(1)(b).

testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing is the fundamental measures for the maintenance of security.

The GDPR highlights that risk assessment for the appropriate level of security, in particular the risks that are presented by processing from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed must be taken into account.[26] A personal data breach is defined under the GDPR as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."[27]

It is important to note that the GDPR only applies to breaches related to personal data. In other words, the GDPR does not apply if the breach does not affect any outcome regarding data protection. As reminded by Article 29 Data Protection Working Party (hereinafter the WP29) "*whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches*."[28]

Considering the problem surrounding the definition of "personal data breach", the WP29 attempts to provide further guidance.[29] According to the WP29, "destruction" of personal data covers situations where the data no longer exists, or no longer exists in a form that is of any use to the controller; damage is defined where personal data has been altered, corrupted, or is no longer complete; loss should be interpreted as the data may still exist, but the controller has lost control or access to it or no longer has it in its possession. The WP29 also explains unauthorised or unlawful processing situations may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing that violates the GDPR.[30]

The WP29 maintains that a breach of confidentiality or integrity is rather clear, on the other hand availability breach may be less evident.[31] Indeed, there is not a blueprint approach or pre-defined template that could be implemented in every circumstance. Each situation and its impacts on personal data must be assessed according to its merits. For instance, a ransomware attack could be qualified as an availability incident and confidentiality breach if a network intrusion has also arisen

26 GDPR Article 32(2).

27 GDPR Article 4(12).

28 Article 29 Data Protection Working Party 'Guidelines on Personal data breach notification under Regulation 2016/679 (Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018)' https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 [accessed 1 March 2021], 7.

29 *Ibid*. 7.

30 *Ibid*. 7.

31 *Ibid*. 8.

during the injection of the malicious software.[32] Nevertheless, depending on the outcome of the breach in terms of confidentiality, integrity, and availability, the data controller is required to engage in notification procedures.

B. The Rationale for Data Breach Notification

The obligation for notification or self-disclosure of breach incidents could be grouped into three categories: regulatory, contractual, and voluntary. This is not an exhaustive list, but rather a guiding taxonomy.

Regulatory types of notification occur when specific legislation mandates breach notification. Contractual types of notification occur when a particular provision of a contract obligates parties to notify each other of any security breaches such as when a cybersecurity insurance could require the insurer or insured to report a breach of this kind. Voluntary types of notification occur when an entity exempted from regulatory requirements chooses to notify relevant stakeholders of any breach to maintain their corporate reputation.[33]

The circumstances that would trigger a breach notification are not limited with the aforementioned cases. For instance, a borrower who has been a victim of cyber-attack might be compelled to inform such an incident to the creditor if the incident has an impact on the business of the borrower and affects the repayment of the credit. Similarly, the creditor might be obliged to notify the third parties who would surrogate the credit. In such cases, the content, format and scope of the notification or the level of transparency will be determined according to the actual contract or service level agreement between the parties.

Notwithstanding the type of notification, the primary objective of the breach notification requirement is to prevent or mitigate all adverse effects or damage

32 *Ibid*. 9; Ransomware is a global threat and such malicious software has different types and forms. For the implications of a ransomware attack on data protection, there is a need to conduct computer forensics alongside network forensics. Depending on the logs of inbound and outbound network at the timeframe when the ransomware code was running, there could be different outcomes. For a detailed examination of different possibilities see EDPB '*Guidelines on Examples regarding Data Breach Notification Adopted on 14 January 2021 Version 1.0*' https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf [accessed 1 March 2021], 7-13; A ransomware could also expose the entity to their customer. For instance, a ransomware operation known as 'Clop' is applying maximum pressure on victims by emailing their customers and asking them to demand a ransom payment to protect their privacy. See, https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/ [accessed 7 April 2021]

33 Voluntary notification is a quite complex issue. As highlighted by Determann "*Even where notices are not legally required, companies sometimes issue notices anyway either because they are not sure whether a notice requirement applies, because they consider notification beneficial from a customer or public relations perspective or because they want to help potentially affected data subjects to mitigate risks, harm and damages claims. Such voluntary disclosures can be helpful, but they can also backfire and provoke over-reactions and unnecessary hassles for data subjects. For example, if a company issues a voluntary disclosure regarding weakness of systems hosting credit card numbers, credit card holders may be induced to cancel credit cards and make filings with credit bureaus, even if there is no concrete indication of an increased potential for abuse.*". See Lothar Determann, *Determann's Field Guide to Data Privacy Law (Fourth Edition)* (Edward Elgar 2020), 5.50.

emanating from a data security incident.[34] This enables the data subjects to take any remedial measures, e.g., changing passwords and cancelling credit cards.[35]

The European Commission has stated in its impact assessment report of the GDPR, "*breach notifications provide a systematic feedback about the actual risk and the actual weaknesses of existing security measures; they enable authorities and consumers to assess the relative capabilities of data controllers with respect to data security; they force data controllers to assess and understand their own situation regarding security measures*".[36]

As underlined by GPDR, a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.[37]

Breach notification triggers the mechanism of accountability, liability against data subjects, business partners, and most importantly, responsibility against data protection authorities. The breach notification requirement imposes a level of transparency on data controllers and makes them crystal clear about their data protection policies and practices. Overall, cybersecurity investment has become widely accepted and increasingly part of standard business practices as cybersecurity incidents have cost companies greatly. Notably, the international technical standards, such as ISO 27001, have been the catalyst for the institutionalization of data security breach management.

As highlighted by the European Union Agency for Cybersecurity (hereinafter ENISA), the cost of reacting to a security breach is usually higher than the cost of adequately addressing the issue proactively.[38] In the same context, it is maintained that "*[e]enterprises are increasingly realizing that it is more cost-effective to include cybersecurity as part of the overall system development lifecycle and rigorously test systems for vulnerabilities, as opposed to trying to fix the aftermath of a cybersecurity breach*".[39]

34 GDPR Recital 85.

35 Lambert (n 2) 305.

36 European Commission, '*Commission Staff Working Paper SEC(2012) 72 final - Impact Assessment accompanying the General Data Protection Regulation*' https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf [accessed 1 March 2021], 100.

37 GDPR Recital 85.

38 ENISA, '*Guidelines for Securing the Internet of Things*' https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things [accessed 1 March 2021], 39.

39 Andrew Gorecki, *Cyber Breach Response That Actually Works* (Wiley 2020), p. 21.

C. Notification of a Personal Data Breach to the Supervisory Authority

Article 33 of the GDPR prescribes an extensive rule for notification of a personal data breach to the supervisory authority. As soon as the controller becomes aware that a personal data breach has occurred, the controller is required to notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

It is important to note that the key for notification is awareness of the personal data breach, not the occurrence of the incident. The WP29 interprets the expression of awareness as having become aware "*when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.*"[40] The standard triggering data notification of a breach is a reasonable degree of certainty.[41] The determination of when an organisation is aware of a breach is potentially critical for legal liability.

The core task of the data controller is conducting an internal evaluation of the event. In this regard, the data controller should ascertain that all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to promptly inform the supervisory authority.[42] As highlighted by the WP29, "*a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it on time.*" [43] Considering these obligations, to emphasise the standard needs to be interpreted narrowly rather than leaving a wide discretion to the data controller.

The data controller could be aware of the data breach through different channels. For instance, the data processor or one of the business partners within the supply chain of the controller could be aware of the breach and warn the controller. Another possibility is that a data subject or any third party could alert the data controller about a breach.

Similarly, the data controller could be aware of the breach in the context of a bug bounty programme or continuous red teaming process.[44] Such programmes invite third-party security researchers to discover any problems, vulnerabilities, or bugs of a given information system as per specific instructions.[45] Lastly, there are illegal dark

40 The WP29 (n 28) 10-11.

41 *Ibid*. 12.

42 GDPR Recital 87.

43 The WP29 (n 28) 6.

44 For example, EDPB, '*Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR Adopted on 09 November 2020*' https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_bindingdecision01_2020_en.pdf [accessed 1 March 2021].

45 The bug bounty could be limited. For instance, the companies could require the researchers to refrain from denial-of-service attacks, spamming, brute-force attacks, social engineering (including phishing) of staff or volunteers, any physical attempts against property or data centers, using scanners or automated tools to find vulnerabilities. Any researcher, who exceed such limits, might face legal and criminal actions.

web markets whereby stolen personal data are sold or exchanged. There are security researchers who scan such networks and deliver intelligence reports regularly to the relevant data controllers.

Public authorities, such as cybersecurity agents or the competent computer security incident response teams could also notify the data controllers about suspicion of a breach. Regardless of the channel of notification, the main duty of the controller is to take such intelligence seriously and initiate an efficient investigation accordingly.

The complexity of IT systems, the diversity of the hardware and software deployed, and the proliferation of providers/suppliers could lead to an investigation of a breach to be concluded speedily. The WP29 maintains that during the period of investigation the controller may not be deemed as being "aware".[46] The data controller, nevertheless, must launch an inquiry and be ascertained with a reasonable degree of certainty about whether a breach has taken place.

Article 33 also provides that where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay. The WP29 exemplifies such a scenario as "bundled" notification multiple, similar confidentiality breaches over a short period affecting large numbers of data subjects in the same way.[47]

On the other hand, the controller is exempted from notification if it can demonstrate as per the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. To reach such a conclusion, one must assess impacts and document the underlying evaluation of such a decision as per the accountability principle.

Notification to the supervisory authority requires qualified correspondence and subject to strict formal requirements. According to Article 33(4), the controller is required to (a) describe the nature of the personal data breach including where possible, the categories and the approximate number of data subjects concerned and the categories and the approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or another contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In general, the data controller is expected to conduct a comprehensive forensics investigation, scrutinize the impact of a data breach, map out the individuals and

46 The WP29 (n 28) 11.

47 *Ibid*. 16.

data affected, establish an active channel of communication with the supervisory authority, make an impact assessment of the prospective effect of the breach, and document concrete actions taken for addressing the breach.

Considering the variety and volume of information to be compiled, the GDPR leaves the door open for data controllers for submitting further documentation. According to Article 33(4) of the GDPR, where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without further delay. As highlighted by the WP29, "*the focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.*"[48]

Within this context, the WP29 underlines that where precise information is not available (e.g., exact number of data subjects affected), this should not be a barrier to timely execute breach notification. The WP29 emphasizes that the focus of the notification requirement to the supervisory authority is "*to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority.*"[49]

In all situations, the data controller is obligated to document in detail. Such documentation must involve three main elements: (1) the facts relating to the personal data breach; (2) the effects of the breach; (3) the remedial action taken. Furthermore, the GDPR mandates that the documentation must be precise and well-structured so that it enables the supervisory authority to verify compliance with Article 33 of the GDPR.

Such requirements are minimum and should be included at the notification at least. In accordance with the merits of the incident and the sector-specific or data-specific risks, most importantly, as per the accountability principle, the level of documentation and the substance of such documentation could vary among the data controllers.

Indeed, the most prominent obligation deriving from the principle of accountability is to have effective warning mechanisms. In a digitalised world where all accountability tools are in operation, is it difficult to bury any evidence? If all works properly, the data generated through security information and event management systems or so-called 'siem' systems, produce rock-solid evidence. Automatic notification systems are also becoming increasingly prevalent in the context of stopping data breaches.

D. Communication of a Personal Data Breach to the Data Subject

If a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, another procedure is triggered in addition to the notification to the supervisory authority: communication of the breach to data subjects. Both Articles 33

48 *Ibid*. 5.

49 *Ibid*. 15.

and 34 use the same wording for pressing the buttons of notification, i.e., the personal data breach's potential or actual "*risk to the rights and freedoms of natural persons*". However, despite similar wording, the burden of triggering notification as per Article 34 is higher.

In Article 34, every potential breach requires notification to the supervisory authority but only high-risk scenarios necessitate communication to data subjects. The reason for this distinction is explained by the WP29 as protecting individuals from unnecessary notification fatigue.[50] In contrast to a notification to the supervisory authority, there is no precise time limit for communication to the data subject.

Considering the consequences of a data breach, Article 34 of the GDPR mandates that such communication shall be made without undue delay. As highlighted by the WP29, "*the focus of any breach response plan should be on protecting individuals and their personal data*."[51] The threshold for such a notification, in this regard, will be determined in accordance with the merits of the breach, the type of the data (e.g., sensitive data), and the severity of the breach.

The rationale to communicate a data breach to the relevant data subject is to allow the subject to take necessary precautions.[52] Therefore, the GDPR underlines that such communications to data subjects should be made reasonably feasible as soon as possible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law enforcement authorities.[53] The WP29 states that if justified and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals as long as it does not prejudice such investigations.[54] In such situations, communication is initiated at a later date to prevent interference in ongoing investigations.

As explained within the GDPR, the need to mitigate an immediate risk of damage would call for instantaneous communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.[55] The GDPR also states that an exception to a notification without undue delay may occur if the nature and gravity of the personal data breach scenario warrant it.[56] Hence, what is meant by "*without undue delay*" will vary in different scenarios.

50 *Ibid*. 20; For examples to distinguish between risk and high risk to the rights and freedoms of individuals see *ibid*. 31.

51 *Ibid*. 5.

52 GDPR Recital 86.

53 GDPR Recital 86.

54 The WP29 (n 28) 21.

55 GDPR Recital 86.

56 GDPR Recital 87.

Article 34 also follows the same methodology adopted by Article 33 terms of the content of the communication. It is likewise a qualified correspondence. Article 33(2) of the GDPR mandates that such communication should describe in clear and plain language the nature of the personal data breach and contain at least the information and measures such as (a) the name and contact details of the data protection officer or other contact points where more information can be obtained; (b) the likely consequences of the personal data breach; (c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The GDPR also leaves the door open for non-notification if certain conditions are met. Article 34(3) of the GDPR lays down three exemptions where communication with the data subject is not necessary. The conditions for exemptions need to be interpreted narrowly. As pointed out by the WP29, while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk might have to be re-evaluated.[57]

The first exemption of communication is a technical one. If a controller implements appropriate technical and organisational protection measures, and those measures are applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption, there is no need for communication. As highlighted by WP, in such cases, nevertheless there could be need for notification if there are problems in terms of availability of personal data, e.g., the controller has no adequate backups.[58]

Other scenarios where a notification obligation would occur is when the risk to the rights and freedoms of a natural person may change. For example, this may occur when a backup exists but considering the length of time taken to restore the data from that backup and the effect the lack of availability has on individuals, or encryption key is compromised.[59]

Nevertheless, this exemption highlights the importance of privacy by design approach and the law rewards data controllers, who have adopted such an attitude by freeing them from a major burden. The use of encryption, in this regard, is a meaningful tool.

The second exemption is a risk-based one. If a controller takes subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise, there is no need for communication. This exemption is in line

57 The WP29 (n 28) 19.

58 *Ibid*. 18.

59 *Ibid*. 19.

with the general rule for notification, which is the personal data breach most likely to result in a risk to the rights and freedoms of natural persons.

The third exemption is a practical one. If the communication to the data subject would involve disproportionate effort, there is no need for individual correspondence with data subjects. Rather in such cases, the data controller is required to make a public communication or similar measure whereby the data subjects are informed in an equally effective manner. The WP29 advises that controllers should choose the means that maximizes the chance of accurately communicating information to all affected individuals.[60]

The decision for a public announcement of a data breach is a quite-complex issue. The GDPR reminds that the data breach rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.[61] Considering the problems surrounding digital investigations, due consideration should be given to the announcement of disclosure to the general public to avoid the destruction of evidence and prevention of identification of perpetrators.

The determination of the risk remains at the epicentre of the notification process.[62] The GDPR stresses that the likelihood and severity of the risk to the rights and freedoms of the data subject must be determined by reference to the nature, scope, context, and purposes of the processing.[63] Likewise, the risk must be weighed based on an objective assessment, i.e., whether data processing operations involve a risk or a high risk. The WP29, in the same direction, highlights that "*where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify*".[64]

60 *Ibid*. 21.

61 GDPR Recital 88.

62 GDPR elaborates different outcomes of the risks to the rights and freedoms of natural persons. Accordingly, the varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects. See GDPR Recital 75.

63 GDPR Recital 76.

64 The WP29 (n 28) 26; For a detailed guidance about the determination of the risk see also ENISA, '*Recommendations for a methodology of the assessment of severity of personal data breaches*' https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport [accessed 1 March 2021].

Article 34(4) of the GDPR confers a wide margin of discretion to the supervisory authorities having considered the likelihood of the personal data breach resulting in a high risk could either require the controllers to communicate to the data subjects if they have not already or decide that the conditions of exemptions are justified. Article 58 also gives supervisory authorities the power to order a controller to communicate personal data breaches to data subjects.

The GDPR also empowers the European Data Protection Board (hereinafter the EDPB) with respect to data breach procedures. According to Article 70, the Board is entitled to issue guidelines, recommendations, and best practices for establishing personal data breaches and determining undue delay and for the particular circumstances in which a controller or a processor is required to notify those affected by personal data breaches as well as for the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons.

F. The Status of Joint Controller

According to Article 26 of the GDPR, where two or more controllers jointly determine the purposes and means of processing, they are regarded as joint controllers. The GDPR transparently mandates the joint controllers to determine their respective responsibilities for compliance with the obligations. The GDPR underlines that the protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors and the monitoring and measures of supervisory authorities require a clear allocation of the responsibilities, including where a controller determines the purposes and means of processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.[65]

Breach notification obligation necessitates the fulfilment of organized and synchronised action. The WP29 suggests that contractual arrangements between joint controllers include provisions that determine which controller will take the lead on or be responsible for compliance with the breach notification obligations of the GDPR.[66]

G. The Status of Data Processor

A data breach can also take place throughout the services of a data processor. Article 28 of GPDR mandates that processing by a processor must be governed by a contract or legal act. Such a contract or legal act, among other things, must stipulate, in particular that the processor assists the controller in ensuring compliance with the obligations under Articles 32 to 36 taking into account the nature of processing and the information available to the processor.

65 GDPR Recital 79.

66 The WP29 (n 28) 13.

Besides Article 28, Article 33 of the GDPR also imposes a general obligation on the data processors for notification of the breach. According to Article 33(2), the processor is required to notify the controller without undue delay after becoming aware of a personal data breach. The data controller, after being notified by the processor and henceforth becoming aware of the breach, will respectively notify the competent supervisory authority or the data subject if needed.

Two issues must be addressed in the event of the breach within the processor's jurisdiction. Firstly, who should carry out the whole examination, the controller or the processor? Secondly, when will the 72-hour countdown regarding awareness and required notification to the relevant authorities begin?

The WP29 maintains that the processor is not required to determine to assess the likelihood of risk emanating from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach.[67] The processor only needs to ascertain that a breach occurred and notify the controller accordingly. Therefore, in principle, the controller should be deemed as "aware" once the processor notifies the breach.[68]

The GDPR does not provide an explicit time limit within which the processor must alert the controller, but only states it must do so "*without undue delay*". The WP29 recommends the processor promptly notifies the controller, with further information about the breach providing in phases as more details become available. The processor must assist the controller to meet the notification requirements of the supervisory authority within 72 hours.[69] Where the processor provides services to multiple controllers that are all influenced by the same incident, the processor will have to report the details of the incident to each controller.[70]

The lack of an explicit statutory deadline for a data processor may contribute to inconsistent practices. It could be argued that the lack of an explicit mandate under the GPDR could open the doors for misuse. Indeed, as per Article 28 of the GPDR, where processing is to be carried out on behalf of a controller, the controller can only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. The data controller, henceforth, cannot avoid responsibility on the grounds of intentional belated notification from the data processor.

67 *Ibid*. 13.

68 *Ibid*. 13.

69 *Ibid*. 14.

70 *Ibid*. 14.

H. Administrative Fines

Deficiencies in data security maintenance, the improper appraisal of risk ratings, the failure to respond in a timely or improper manner while notifying a breach, the failure of communication of data breach to the data subjects or inadequate reporting could give rise to heavy sanctions. Data controllers who violate their obligations under Article 32 to 34 of the GDPR are subject to administrative fines up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Article 83 of the GPDR lays down general conditions for imposing administrative fines and requires that each supervisory authority ensures that the imposition of administrative fines in each case must be effective, proportionate, and dissuasive.[71] In addition to this general requirement, the GDPR also requires that when deciding on whether to impose an administrative fine or deciding on the amount of the administrative fine in each case, due regard be given to the following:

(1) the nature, gravity, and duration of the infringement;

(2) the intentional or negligent character of the infringement;

(3) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(4) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them;

(5) any relevant previous infringements by the controller or processor;

(6) the degree of cooperation with the supervisory authority, to remedy the infringement and mitigate possible adverse effects of the infringement;

(7) the categories of the personal data affected by the infringement;

(8) how the infringement became known to the supervisory authority, in particular and if so, to what extent the controller or processor notified the infringement;

(9) where measures have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(10) adherence to approved codes of conduct or approved certification mechanisms;

71 For a comprehensive review of substance of administrative fines see, The WP29, '*Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 Adopted on 3 October 2017*' http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889; For instance, German data protection authorities has published a detailed methodology for determination of administrative fines. See, '*Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen*', https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf [accessed 1 March 2021].

(11) any other aggravating or mitigating factor applicable to the circumstances of the case such as financial benefits gained, or losses avoided directly or indirectly from the infringement.

Article 58 of the GPDR considers allowing regulators to issue reprimands is a core investigative power that each supervisory authority must have. It is noteworthy that in the case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.[72]

I. Evaluation of the GDPR's Rules and Procedures

The main objective of the GDPR is to prevent potential risks and prejudices rather than imposing sanctions due to violations.[73] It is argued that "*the security obligations are designed not only to prevent data breaches and cyberattacks but also to achieve the broader goal of ensuring the functioning of ICT systems, their interoperability and, more in general, their reliability*".[74]

This innovation of the GDPR has been a breakthrough in the EU, and thousands of violations have been reported to the data protection authorities since 2008. The data protection authorities have also levied severe sanctions for different data security violations. For instance, in Germany for the period from 25 May 2018 to 27 January 2021 77,747 personal data breaches were reported to the supervisory authorities while fines totalling 69,085,000 Euros were imposed.[75] Similarly, in the Netherlands, in the same period, 66,527 personal data breaches were notified while fines with a total value of 2,540,000 Euros were levied.

Total number of personal data breaches notified per jurisdiction for the period from 25 May 2018 to 27 January 2021 inclusive[76]	
Germany	77.747
Netherlands	66.527
United Kingdom	30.536
Denmark	18.938
Ireland	17.131

The GDPR creates a specific accountability scheme for the maintenance of data security, which adds another layer to the general accountability obligation deriving

72 GDPR Recital 148.

73 Alessandro Mantelero, *et al*., '*The common EU approach to personal data and cybersecurity regulation*', 1 International Journal of Law and Information Technology 1(2021) 3.

74 *Ibid.*, 4.

75 DLA Piper, '*GDPR fines and data breach survey: January 2021*' https://www.dlapiper.com/en/poland/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/ [accessed 1 March 2021], 9.

76 *Ibid.*

from Article 5, i.e., the principles relating to the processing of personal data. Irrespective of notification to the supervisory authority or communication to the data subjects, the data controller is required to document any personal data breaches comprising the facts relating to the personal data breach, its effects, and the remedial action taken. Any notification or communication should be accompanied by a detailed forensic report and mitigation or remediation plan. The WP29 recommends that the controller document its reasoning for the decisions taken in response to a breach.[77]

As explained, as per Article 33(5) of the GDPR, the controller needs to record details of the breach including its causes, what took place, and the personal data affected. It should also include the effects and consequences of the breach along with the remedial action taken by the controller. The GDPR explains that when setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach including whether personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse.[78]

The notification of the breach to the relevant data protection authority and data subjects respectively needs an internal assessment by the data controller. The primary factor that determines the overall process and success of the fulfilment of the legal obligations is the accountability mechanisms put in place by the data controller before the incident of the breach.[79]

It could be argued that the documentation requirements are high and the time for the notification (72 hours) is quite short whereas the liability compared to the requirements is disproportional. Indeed, the GDPR establishes a sustainable data protection system with various tools and instruments from code of conduct to certifications. The main paradigm of this data protection eco-system is the accountability approach.[80]

The GDPR's detailed data breach notification rules and the short timeframe for the GDPR's detailed data breach regulatory rules and the short timeframe for notification are the result of companies historically hiding breaches for a long time.[81] GPDR "*seeks to curb the culture of secrecy by first holding the controllers accountable for the safety of the data, second, having them react quickly to such attacks, and lastly requiring the controller to be transparent if it occurs, in order to increase accountability*".[82]

77 The WP29 (n 28) 27.

78 GDPR Recital 88.

79 For example, incident detection and reporting, incident notification to organization (e.g., notification or demand from hacker; posting online; etc.), internal notification(s), team notifications, risk assessment, impact assessments, disciplinary action, hacker relation action, data protection supervisory authority external breach notification, individual data subject breach notification, customer breach notification. See, Lambert (n 2) 312.

80 Mantelero, *et al*. (n 73) 4.

81 Sanjay Sharma, *Data Privacy and GDPR Handbook* (Wiley 2020) 107.

82 *Ibid*.

Yet, there are significant problems in practice while implementing the data breach notification. The rules introduced by the GPDR are arguably "*extremely broad and stringent requirements are paired up with extremely broad and vague exceptions*".[83] According to an analysis of breach notifications received from various areas within the public and private sector conducted by the Data Protection Commissioner of Ireland, late notifications, difficulty in assessing risk ratings, failure to communicate a breach to data subjects, repeating breach notifications, and inadequate reporting are the prominent mistakes of the data controllers and the major problems in the practice.[84]

IV. The Turkish Law

A. Breach Notification Rules Outside of the Turkish DP Law

Turkey does not have a general network and information security law or umbrella legislation on cybersecurity. The legal framework is relatively fragmented when it comes to reporting security breaches. The Turkish government has announced that it will transpose the EU NIS Directive into its national law to defragment the legal framework.[85]

Turkey's cybersecurity law is scattered throughout different legal frameworks. In 2016, a distinct provision was incorporated into Section 11 of Article 60 of the Electronic Communication Law no. 6698, and the Turkish Information and Communication Technologies Authority ("the ICTA") was given a unique authority to compel public institutions, organisations, real and legal persons to take all kind of precautions against cyber-attacks, and to establish deterrence against such attacks. The ICTA is authorized to levy sanctions from 1.000 to 1.000.000 Turkish Liras if the necessary measures are not adopted by the relevant entity or person.[86]

The ICTA constantly traces the cybersecurity incidents through publicly available and private forums and mediums, e.g., security bulletins and deep web forums, audits the companies with respect to specific cyber threats, establishes coordination between public and private entities and stakeholders, and alarms the entities for trending threats and technical vulnerabilities.

83 Determann (n 33) 5.44.

84 The Data Protection Commission (DPC), '*A Practical Guide to Personal Data Breach Notifications under the GDPR*', https://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide [accessed 1 March 2021], 2.

85 Presidency of the Republic of Turkey, '*The Eleventh Development Plan (2019-2023)*' https://www.sbb.gov.tr/wp-content/uploads/2020/03/On_BirinciPLan_ingilizce_SonBaski.pdf [accessed 1 March 2021].

86 This power granted to the ICTA is quite wide and vague. Nevertheless, the Turkish Constitutional Court has ruled that such a power is related to the maintenance of public order at cyber space and has rejected the request for annulment of this aforementioned provision. The Court held that "*Undoubtedly, ensuring cyber security is among the duties assigned to the State in ensuring that individuals live in safety.*" See the Turkish Constitutional Court, Case No: 2017/16, Decision No: 2019/64, Decision Date: 24.07.2019.

Other than the telecommunication sector, a general notification requirement is also in effect for the banking sector. According to Article 38 of Regulation on Network and Information Security in Electronic Communications Sector[87] operators in the electronic communication sector are obliged to notify network and information security violations, which affect 5% of their subscribers. These notifications and other similar notifications to the ICTA are expected to include the measures that are to be taken against these breaches.

Besides the telecommunication sector, a general notification requirement is currently valid for the banking sector. Pursuant to Article 18(5) of the Regulation on Banks' Information Systems and Electronic Banking Services which is overseen by the Turkish Banking Regulation and Supervision Agency, banks are obliged to notify their customers in case of a cyber-attack resulting in breach or disclosure of data or personal data.[88] Similar obligation has likewise been laid down for the notification of cyber-attacks resulting in any serious outage or disruption. As per Article 6, such incidents are required to be reported to the national cybersecurity incident response team.

Similar notification requirements exist under different laws such as By-Law on Information Systems Management of Capital Markets Board of Turkey,[89] Regulation on Information Security in Industrial Control Systems Used in Energy Sector,[90] Regulation on Specific Principles for Safety of Nuclear Power Plants[91], and Internet Domain Names Regulation[92]. The common requirement under these regulations is to notify the customers and the competent authority in case of cyber threats and risks.

Furthermore, commercial regulations could lead to a notification of a security breach. According to Article 82 of the Turkish Commercial Law, merchants, who must act prudently, need to keep their books accurately and ensure the security of their documents. Pursuant to Section 7 of Article 82, if the books and documents of a merchant are lost during the statutory retention term due to a disaster such as fire, flood, earthquake or theft, the merchant is entitled to request a document from the competent court within fifteen days from the date of learning about the loss.

If fiscal data is compromised, a notification to the tax authorities could enter into question. According to Article 7 of the Electronic Book General Communiqué,[93] if a force majeure in the context of the Turkish Tax Procedure Law occurs which affects

87 OJ 13.07.2014/29059.

88 OJ 15.03.2020/31069.

89 OJ 05.01.2018/30292.

90 OJ 13.07.2017/30123.

91 OJ 17.10.2008/27027.

92 OJ 07.11.2010/27752. See also, Internet Domain Names Communiqué, OJ 21.08.2013/28742.

93 OJ 13.12.2011/28141.

e-books, e-book keepers need to apply to the Turkish Revenue Administration within 15 days as of the date of the event and demand for a certificate of loss. It is noteworthy that cyber-attacks could likewise constitute a force majeure situation.

As discussed under Section III, the breach notification could also emanate from a contractual obligation. Cyber risk insurances are classical examples of such contracts that encapsulate unique notification rules and procedures. According to the ENISA, cyber risk insurances are contracts dealing with a broad range of risks in cyberspace and covers matters like liability issues, property loss and theft, data damage, loss of income from network outage, and computer failures or website defacement.[94]

The proliferation of cybersecurity and data protection regulations has boosted demand for such insurance contracts and is indeed regarded as demand-side triggers.[95] Cyber risk insurances have become popular in Turkey in diverse sectors and by various entities. Even though cyber risk insurances do not cover all possible cyber threats, which indeed would be impractical considering the evolving landscape of cyberspace and hyper-connectivity,[96] they at least stand for essential tools for addressing prominent threats.

According to Article 1475 of the Turkish Commercial Law, the insured is obliged to notify the insurer within ten days of a breach event that may give rise to its liability.[97] In addition, the policyholder is obliged to notify the insurer without delay when it becomes aware of the materialisation of the risk as per Article 1446 of the Turkish Commercial Law.

Besides notification obligation, the Turkish Commercial Law also mandates a detailed documentation obligation. Pursuant to Article 1447, after the materialisation of the risk, the policyholder must, following the contract or upon the insurer's request, provide all information and documents which are necessary for determining the extent of the risk, and indemnity might be expected from the policyholder to the insurer within a reasonable period. Having an incident response and notification plan, in this regard, is considered the primary element of a cyber-risk insurance contract.[98]

94 ENISA, '*Incentives and barriers of the cyber insurance market in Europe*' https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport [accessed 1 March 2021], 8.

95 Kirsty Middleton, Maria Kazamia, '*Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concerns*' in Pierpaolo Marano, Ioannis Rokas and Peter Kochenburger (eds), *The "Dematerialized" Insurance - Distance Selling and Cyber Risks from an International Perspective* (Springer 2016), 187.

96 It would be beyond scope of this article to address all problems with regard to cyber insurances. Nevertheless, it is argued that "*[c]overing cyber risks could put companies in a challenging situation in which a traditional approach to risk aggregation might prove inadequate. Companies tend to think of coverage as their only cyber insurance product. They could establish a robust infrastructure by building partnerships with all the stakeholders. Companies should adopt a broader view of risk prevention through partnerships and aiming at insuring rather than just insurance.*" Bernardo Nicoletti, *Insurance 4.0: Benefits and Challenges of Digital Transformation* (Palgrave Macmillan 2021), 87.

97 This provision is an imperative provision that cannot be altered to the detriment of the insured as regulated under Article 1486(2) of the Turkish Commercial Law.

98 Ahmet Karayazgan, *Hukuki Yönüyle Sİber Riskin Sigorta ve Reasüransı* (Legal. 2020), 147.

The maintenance of quality and reliability of data is the most critical challenge for cyber risk insurances. To overcome such restraint, insurers could mandate the deployment of a cyber-agent within the insured information systems. Such agents monitor the operation of all systems, keep records of any security event and incidents and report them when needed. The automatization of security events and incidents is a breakthrough development as it eliminates the risk of under-reporting and hiding the evidence.[99]

There is a misconception that cyber insurance policies are extremely expensive and the amount that firms have to pay in premiums and deductibles for insurance coverage is comparable to the amount a firm pays out of pocket to cover the costs of a breach.[100] Nevertheless, cyber risk insurances are evolving into efficient instruments for enhancing data breach notification mechanisms. Contractual obligations may be more effective than regulatory obligations when it comes to the disclosure of breaches. Moreover, cyber insurance monetary payments may be used by authorities to find bad actors. The payments in the scope of cyber insurances are significant pieces of evidence while identifying data breaches that could guide the data protection authorities.

What if such insurances are misused to defraud the insurance process? Indeed, if the fraud includes manipulation with regard to the personal data breach, then the same controller will encounter the scrutiny and sanctions of the relevant data protection authority. Hence, the co-existence of penalties and fines creates a kind of check-balance system for cyber insurance frauds.

Aside from the security-related provisions, a general rule under the Turkish Criminal Law no. 5237 could also indirectly trigger a breach notification. Article 279 of the Criminal Law mandates that any public officer who fails to report an offense (which requires a public investigation and prosecution) or delays in reporting such offence to the relevant authority after becoming aware of such offence in the course of his duty will be sentenced to a penalty of imprisonment for a term of six months to two years. Taking into consideration the data protection-related crimes fall under the Criminal Law, it could be the case that a data breach could be discovered ex officio by the public officers.[101]

B. The Examination of the Turkish Data Protection Law

Turkey has adopted its first general data protection law in 2016. Moreover, an independent supervisory authority, so-called the Turkish Data Protection Authority

99 It is argued that the insurance market suffers with a handicap because many companies are reluctant to share information in general. See, Centre for Maritime Law, '*Maritime Industry: Cyber-Risk & Security*' https://cmlnluo.law.blog/2020/01/05/maritime-industry-cyber-risk-security/ [accessed 1 March 2021]; Kevin DiGrazia, '*Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach*' (2018) 13 Journal of Business & Technology Law 225, 260.

100 *Ibid*. 260.

101 Türkay Henkoğlu, *Adli Bilişim - Dijital Delillerin Elde Edilmesi ve Analizi* (Pusula 2014),79.

("the DP Authority") was established for overseeing the implementation of the DP Law. The central decision-making body of the DP Authority is the Turkish Data Protection Board (hereinafter the DP Board).

Although the DP Law is essentially modelled after the Directive 95/46/EC, it has unique rules tailored in accordance with Turkish law and policy. The Turkish government has also announced that it will bring the DP Law in line with the GDPR over time.

In 2019, the DP Board issued a decision that laid down the procedures and principles of personal data breach notification.[102] The DP Board maintains that the purpose of the notification to the DP Board and the data subjects affected by the breach is to ensure that measures are taken to prevent or mitigate the adverse consequences of such violations.[103]

a. What constitutes a data breach according to the Turkish DP Law?

The DP Law, in parallel with Directive 95/46/EC, lays down a general data security obligation on the data controllers. According to Article 12(1) of the DP Law, the controllers must take all the necessary technical and administrative measures to provide a sufficient level of security to prevent unlawful processing of personal data, restrict unlawful access to personal data, and ensure retention of personal data.

The DP Board explains that appropriate measures will be determined on a case-by-case basis which prevents the application of a single model for data security.[104] The DP Board, in this regard, stipulates that the appropriate measures must be determined by taking into account the nature of the work performed by the data controller and the personal data protection are important as well as the size and turnover of the company.

The DP Law, in contrast to Directive 95/46EC, has introduced a general breach notification obligation. According to Article 12(5) of the DP Law, in case the processed data are obtained by other parties through unlawful methods, the controller is under the legal obligation to notify the data subject and the DP Board within the shortest time.

The DP Law does not specifically define rules addressing different types of breaches of security. The general scenario that triggers a breach notification is limited to cases whereby personal data "*obtained by other parties through unlawful*

102 See the DP Board, '*Procedures and Principles of Personal Data Breach Notification, Decision No. 2019/10 of 24.01.2019*' https://www.kvkk.gov.tr/Icerik/6647/The-Board-Decision-No-2019-10-of-24-01-2019-about-Procedures-and-Principles-of-Personal-Data-Breach-Notification- [accessed 1 March 2021].

103 *Ibid*.

104 The DP Authority, '*Obligations Concerning Data Security*' https://kvkk.gov.tr/Icerik/6601/Obligations-Concerning-Data-Security- [accessed 1 March 2021].

methods". In other words, the breach notification obligation is only limited to cases where intentional or accidental unlawful access of third parties to a personal data occurs.

What is meant by "*to be obtained by unlawful methods*"? It is argued that unlawfulness should not be interpreted narrowly and limited to only breach of the DP Law.[105] Considering the vastness of the legal framework regulating personal data such as in the Turkish constitution, sector-specific legislations, international agreements, "*to be obtained by unlawful methods*" must be interpreted as violation of any data protection legislation besides the DP Law.[106] This teleological view is indeed reasonable and fits the purpose of the DP Law, which is the protection of fundamental rights and freedoms of people, particularly the right to privacy with respect to processing of personal data.

On the other hand, the type of security breaches that trigger notification procedure must be scrutinised. To recap, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed as per Article 4 of the GPDR. Depending on the outcome of the breach in terms of confidentiality, integrity, and availability, the data controller is required to trigger notification mechanisms pursuant to the GDPR.

It could be argued that according to the DP Law, the notification of a breach will be required only when the confidentiality of personal data is breached. On the other hand, a breach of integrity and most importantly, a breach of availability will not trigger any notification process.

As the WP29 highlights, a loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack which renders personal data unavailable.[107] The WP29 also defines that a security incident resulting in personal data being made unavailable for some time is also a type of breach as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons.[108]

Additionally, under the current version of Article 12 of the DP Law, a security incident leading to destruction, loss, or alteration of personal data or simply an attack on the availability of personal data will not be reported to either the DP Board or data subjects unless the result of such incident allowed third parties to gain access to such

105 Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku 2. Baskı* (Hukuk Akademisi 2019) 419.

106 *Ibid*.

107 The WP29 (n 28) 8.

108 *Ibid*. 8.

data. In other words, breach of confidentiality requires notification whereas integrity and availability do not require any notification.

The DP Board requires data controllers to explain the impact of a data breach while triggering the notification process. Data controllers are expected to explain the extent of the breach and how it has affected confidentiality, integrity, and availability of personal data. However, such a distinction of different types of security breaches is only articulated under the data breach notification form. It would be against most basic principles of law to the extent the obligations of data controllers strictly regulated under the law through such an administrative form.

Section 5 of Article 12 only mandates notification cases regarding processed data illegally obtained by third parties through unlawful methods. This is the major shortcoming of the Turkish law. There is a need to enhance the normative value of data security under the DP Law by explicitly articulating that confidentiality, integrity, and availability are the main pillars of data security and must be notified if breached.

b. Notification of a personal data breach to the DP Board

What does "shortest time" mean in the context of Article 12(5) of the DP Law? The DP Board has defined the shortest time as requiring an entity to notify within 72 hours after becoming aware of a data breach.

According to the DP law, the key to the notification is awareness, not occurrence. While the DP Board does not provide any guidance with regard to the threshold of awareness, it could be argued that a reasonable degree of certainty is sufficient like in the GPDR. The data controller, in this regard, must launch an inquiry and ascertain with an acceptable degree of certainty whether a breach has taken place.

The DP Board follows the footsteps of the GPDR and mandates that where such notification cannot be achieved within 72 hours, the reasons for the delay should be attached to the notification to be made to the DP Board without further delay. Likewise, the DP Board states that in cases where it is not possible to provide the information simultaneously, this information must be provided gradually without delay.

How shall 72 hours be interpreted? For instance, if a data controller completes all internal procedures within hours and initiates notification procedures at the end of the deadline, is it still liable for not reporting sooner? While the focus of any breach is to protect individuals and their personal data, each case must be evaluated according to its own merits.

Another important topic that needs to be addressed is the scope of application of the DP Law. The DP Law lays down no specific provision for its extraterritorial application.

Yet the DP Board introduces a specific rule that could be applied to a circumstance of extraterritorial application. If data breaches occur through data controllers established abroad and that affects Turkish citizens and entities or if data subjects benefit from the products and services provided within Turkey, these data controllers are required to notify the DP Board and follow the same procedures as domestic companies.

The DP Board has standardised and digitalised the personal data breach notification process to account for domestic and extraterritorial breaches through a standard "Personal Data Breach Notification Form," to be used in all phases of notification. To account for expediency and other challenges, the DP board permits online notification of any data breach.[109]

The notification to supervisory authority is also qualified correspondence which is subject to strict formal requirements. The DP Board requests a broad range of information with respect to various details of the breach, its effects on the data subjects and the data controller, and the measures taken respectively[110] Notably, the DP Board is entitled to announce such breach at its official website or through other methods it deems appropriate where necessary. The discretion remains at the DP Board for publication of such notice.

The DP Board may officially publish breaches on their website or through other methods as deemed necessary. The DP Board's website is a governmental site that is well indexed on search engines and various platforms which bundle breach notifications. Publication of online breaches can turn the spotlight on a data controller and undermine a reputation developed over years. These breaches are also widely distributed as examples within academic works highlighted in legal newsletters and national news coverage and are retained in archives permanently.

The amplification of the breach through multiple channels could ruin the digital identity of a data controller regardless of the size and details of the incident and can create irrecoverable damage to the controller. Therefore, it could be said that the publication of such a breach is the most severe and indirect sanction of a data breach. These outcomes could create a psychological barrier to the notification of breaches. To avoid such a negative public appearance, the data controllers could refrain from notification of a breach.

109 The DP Board, '*Data Breach Notification*' https://ihlalbildirim.kvkk.gov.tr [accessed 1 March 2021].

110 The information to be provided by the data controllers are as follows: (1) The start and end time of the breach, (2) the time when the breach was detected, (3) if the breach is communicated by the data processor to the data controller, the detection time by the processor and the communication time to the controller, (4) the source of the breach and the method of occurrence of the breach, (5) the potential impact of the breach, (6) how the breach was detected, (7) the personal data types affected from the breach, (8) the number of people and total records of data affected from the breach, (9) the personal data group affected from the breach, (10) whether the data subjects are informed with regard to the breach and the details of such communication, (11) whether any domestic or international organization or institution is notified or to be notified with regard to the breach, (12) the possible negative outcomes that data subjects could encounter due to the breach, (13) the effects of the breach on the organization of the data controller, (14) the technical and organizational measures taken by the data controller before and after the breach.

Although the DP Board was notified of 408 breach incidents by January 2021, only 72 of those notified were published on the official website indicating the lack of transparency and objective criteria for the publication of breaches and a shortcoming of Turkish law. The DP Board has not published its criteria for the publication of a data breach.

Examining all the publications, it could be said that the criteria such as the communication of the breach to the data subjects, the extent of the breach and the damage, the number of affected data subjects, the type of personal data, and whether such breach was announced by the data controller himself/herself via any appropriate channel are being used by the DP Board. Nevertheless, to ensure equal treatment, fairness and most substantially, to provide legal certainty, there is a need to lay down an objective criterion for publication of the breaches by the DP Board.[111]

It is noteworthy that the Turkish Criminal Law no. 5237 regulates various data protection-related crimes, e.g., unlawful recording of personal data, illegally obtaining or transferring data, and the failure to destroy data as per the legal requirements. To identify the perpetrators, a data controller besides notifying the DP Board, might need to make a criminal complaint and trigger a criminal investigation.

The criminal investigations must be conducted in full confidentiality. Pursuant to Article 285 of the Turkish Criminal Law, any person who publicly breaches the confidentiality of an investigation is sentenced to a penalty of imprisonment for a term of one to three years as well as incurring judicial fine.

As explained earlier, GDPR underlines that the data breach rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach. If a data controller informs the DP Board about a lodged criminal complaint, the DP Board is required to await the completion of investigation phase before the publication of such breach on its website or through other means.

b. Communication of a Personal Data Breach to the Data Subjects

The DP Board has clarified the rules with respect to the communication of the breach to the data subjects. The persons affected by such data breaches should be informed about the breach in the shortest reasonable period. If the data subject can be reached by mailing address, notification should be made directly. If one cannot

111 The publication of data breaches has also technical consequences. For instance, when a data controller's information systems are infected with a ransomware which encrypts all data and demands a ransom for the decryption key, the absolute confidentiality of the negotiations is vital. An early or untimely publication of a data breach could generate non-recoverable burdens on the data controller and the data controller could lose the only chance of achieving the decryption key.

be reached, notification should be made by appropriate methods such as publication through the data controller's website.[112]

In contrast to the notification to the DP Board, there is no exact time limit for communication of the breach to data subjects. The DP Board requires such communication to be launched in the shortest reasonable period. It is suggested that a similar time limit as already specified while notifying the DP Board (i.e., 72 hours) should be mandated for communication of a personal data breach to the data subjects, preferably a longer time limit.[113]

The DP Board requires the data controllers to establish an efficient communication channel that would enable the data subjects to appraise the full extent of the breach. The DP Board has clarified the minimum content required for breach communications to data subjects based on the GDPR's criteria.[114]

Within this context, the communication is required to describe in clear and plain language the nature of the personal data breach and contain at least the information and measures such as (1) when the breach has occurred, (2) the affected personal data by specifying the categories of personal data (personal data / personal data of special nature), (3) the likely consequences of the personal data breach, (4) the measures taken or proposed to be taken by the controller to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects, (5) the name and contact details of the data protection officer or other contact points, e.g. the full address of the website of the data controller, call centre number, etc., where more information can be obtained by the data subjects.

As discussed previously, in the GDPR while every risk requires notification of the breach to the supervisory authority, only high risk necessitates communication to the data subjects. The data controller is exempted from communicating with data subjects if technical, risk-based or practical grounds justify it. For instance, if the communication to the data subject would require disproportionate effort, there is no need for individual correspondence with data subjects. Similarly, if a controller takes subsequent measures which ensure that high risk to the rights and freedoms of data subjects is no longer likely to materialise, it is exempted from communicating with data subjects in order to prevent individuals from unnecessary notification fatigue.

However, the DP Law differs from the GDPR because it does not provide any such exemptions to data controllers regarding data subject notification. Under the DP law,

112 For instance, as a result of low quality of data or out-of-date communication information, it might not be possible initiate a communication. See, Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu* (On İki Levha 2018), 112.

113 Dülger (n 105) 422.

114 The DP Board, '*Decision No: 2019/271 Date: 18.09.2019*' https://kvkk.gov.tr/Icerik/5547/2019-271 [accessed 1 March 2021].

obligation to communicate the breach in all cases regardless of the nature and scope of the breach, imposes a significant burden on the data controllers. Such burdensome requirements could create psychological barriers to the notification of data breaches. The lack of objective criteria for communication of personal data breach to the data subjects is a shortcoming of the Turkish law.

c. The Status of Data Processors

Pursuant to Article 12(2) of the DP Law, in a case where the processing of personal data is carried out by another natural or legal person on behalf of the data controller, the data controller is jointly responsible with that individual to comply with the regulations. The data controller is expected to conduct the necessary audits or hire a consultant to ensure the implementation of the DP Law provisions.

The DP Board mandates that if the personal data held by the data processor is obtained by others via unlawful methods, the data processor is required to notify the data controller without any delay. The data controller, when notified by the data processor and when it becomes aware of the breach, must initiate the data breach notification process.

Although the DP Board does not set a specific time limit for such notifications from the data processors, the data controller cannot evade responsibility on the grounds of intentional belated notification from the data processor. However, the data controller may seek recourse from the data processor via contractual arrangements if the processor intentionally delays notification.[115]

d. Accountability

The DP law does not articulate a principle of accountability among its general principles. However, the DP Board further mandates that documentation must be available for the DP Board to examine. Nevertheless, the controller is required to document all personal data breaches including the facts relating to the personal data breach, its effects, and the measures taken as specified by the DP Board's decision in 2019.

The DP Board adds another layer to this accountability requirement. The DP Board requires the data controller to prepare a data breach response plan, which must be reviewed regularly. Such a plan must address issues such as to whom the report will be provided, the responsibilities regarding the notification, and the assessment of potential consequences of a data breach.

115 Çekin (n 112) 112.

e. Administrative Fines

The DP Law does not merely regulate an obligation of data security but also sanctions the infringement of this obligation. Under Article 18(1)(b) of the DPL, the Turkish DP Board is entitled to levy an administrative fine of 29.503 TL to 1.966.862 TL[116] on data controllers who fail to fulfil the data security obligations. Therefore, improper notification, late notification, failure to maintain data security, and improper communication of the incident to data subjects could all be subject to a separate or combined administrative fine.

The discretion granted to the DP Board is quite broad. The margin between the lower and upper limit of the administrative fine is a magnitude of sixty-six. Indeed, the Turkish Misdemeanours Law allows administrators to determine fines based on the minimum and maximum limits. Pursuant to Article 17, in such cases, the criteria such as the substance of unfairness level of the committed misdemeanour, the fault, and economic status of the perpetrator need to be taken into account while exercising discretion.

The GDPR states that supervisory authorities should exercise discretion regarding administrative fines. These fines should be based on the nature, gravity, and duration of the infringement, the international character of infringement known to the data protection supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct, and any other aggravating or mitigating factor.[117] Within this context, the DP Law is less-detailed and fails to address all criteria for determination of administrative fines in the GDPR.

The DP Board, as an administrative body subject to public law, must exercise its discretion objectively, specify the level of the unlawfulness of the data breach, and justify its reasons for divergence from the minimum limits of fines through elaborating such reasoning via references to the merits of the case. The failure of such detailed reasoning may create legal uncertainty, which is against the rule of law in a democratic society.

It is noteworthy that similar regulatory authorities such as the ICTA and the Turkish Competition Authority have issued secondary regulations on the implementation of administrative fines which have explicit criteria to be used in the determination of administrative fines. To disperse the clouds of ambiguity and provide legal certainty, the DP Authority needs to issue additional clarification regarding a calculation methodology for administrative fines.

Since actual commencing operation in 2017, the DP Board imposed administrative

116 These amounts are updated annually. The numbers represent the margin to be used in 2021. The amount is equivalent to about 3.924 to 261.555 USD by 18.01.2021.

117 GDPR Recital 148.

fines amounting to approximately 36 Million Turkish Liras. According to the annual report of the DP Authority in 2019, only a total fine of 11 million Turkish Liras was levied due to data breaches.[118] The detailed statistics are as follows:

Table 1: Data Breach Statistics

	2017	2018	2019	2020	2021	Total
Total number of cases	1	28	139	228	17	413
Closed cases	1	24	116	95	0	236
Pending cases	0	4	23	133	17	177
Published breaches	0	4	37	27	2	70

As discussed previously, the Turkish Criminal Law regulates various data protection related crimes. The implementation statistic of these crimes is as follows:

Judicial Statistics 2019[119]

The Crime	Total	Filing a public case	Number of imprisonment sentence decisions	Number of decisions of judicial and administrative fine
Art. 135 - Recording of Personal Data	2987	755	108	2
Art. 136 - Illegally Obtaining or Giving Data	26590	5962	634	27
Art. 138 - Destruction of Data	95	12	1	-

It is noteworthy that the number that has been reported to the DP Board is quite-low. Even, when the judicial statistics are examined with regard to the implementation of personal data-related crimes under the Turkish Criminal Law, there is a significant gap between the DP Law and the Turkish Criminal Law. The reason of avoiding notification of the breaches by the data controllers or in other words, the reasons of notification-phobia needs be queried respectively.

Furthermore, when the decisions adopted by the DP Board in the context of data security are reviewed, there are shortcomings in the implementation of the DP law. As explained, according to the DP law, the key to the notification is awareness, not occurrence. The data controller, in this regard, must launch an inquiry and ascertain with an acceptable degree of certainty whether a breach has taken place.

For instance, the DP Board has chosen to impose an administrative fine on a data controller on the ground of late notification even though the controller has argued

118 The DP Authority, '*2019 Faaliyet Raporu*' https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/c325adf5-5337-4567-95c8-b6b953b745aa.pdf [accessed 1 March 2021].

119 The Turkish Ministry of Justice, '*Judicial Statistics 2019*' https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/1092020162733adalet_ist-2019.pdf [accessed 1 March 2021].

that the delay has derived from the slowness of technical forensic examination (the examination of server and firewall log records).[120] It is learned from this decision that the incident was detected on 28.02.2020 and the DP Board was notified on 04.03.2020 when the forensic investigation was concluded. Nevertheless, this was considered as a late notification by the DP Board.

Undoubtedly, the forensic examination could take a substantial time respecting the volume and variation of the logs to be investigated.[121] The DP Board could have laid down the rules to be respected for digital forensic procedures or refer to either national or international standards of digital forensic; so that the DP Board could have guided the data controllers appropriately. However, the DP Board has failed to lay down an objective criterion for distinguishing occurrence and awareness of a data breach. Notably, such vague decisions, which do not address the technical dimensions adequately, create additional legal and psychological barrier to the notification of breaches.

On the other hand, the DP Board has decided not to impose any administrative fine on a data controller who is operating in the energy sector despite late notification of a data breach.[122] The DP Board has regarded the multi-national structure of the data controller as well as the obstacles in ascertaining and determining the breach notification requirements as legitimate excuses. It is important to note that such inconsistent decisions undermine the principle of equal treatment.

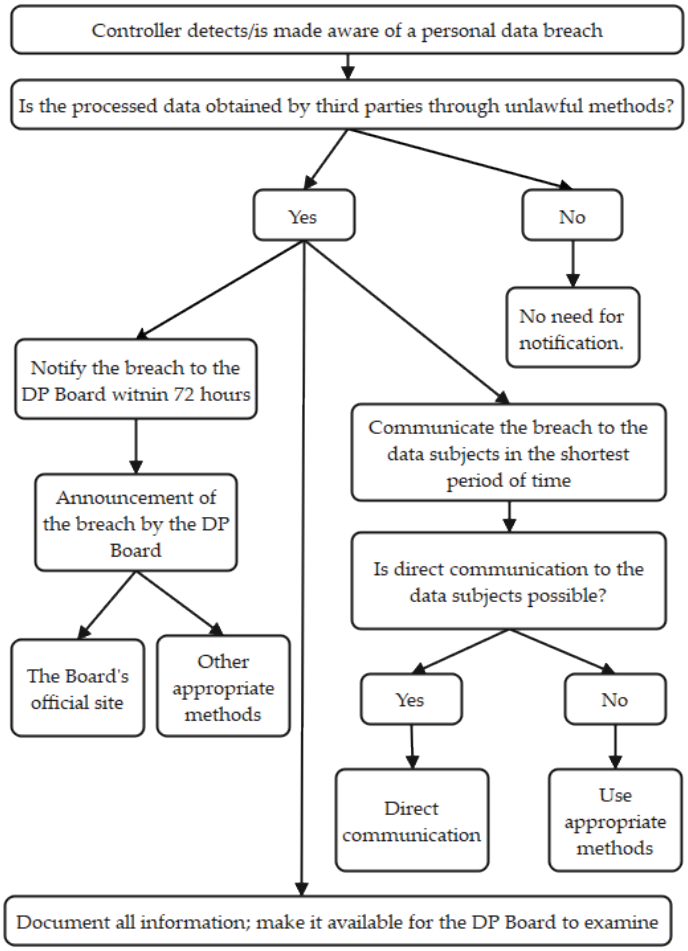
f. The Breach Notification Flowchart

The data breach notification process as per the Turkish DP Law could be summarised as follows:

120 The DP Board, Decision No: 2020/905 Date: 24.11.2020.

121 For a comprehensive review of digital forensics see Grep Gogolin, *Digital Forensics Explained (Second Edition)* (CRC Press 2021).

122 The DP Board, Decision No: 2020/934 Date:08.12.2020.



V. Evaluation of the Findings

The main drawbacks of the DP Law could be categorized under seven groups:

(1) The DP law fails to address all types of security breaches that requires notification

Currently, the DP Law only requires notification of a breach to the data subjects when personal data is obtained by other parties through unlawful methods. To recap, Section 5 of Article 12 is straightforward and only mandates the notification in case the processed data are obtained by third parties through unlawful methods. Hence, there is a need to enhance the normative value of data security under the DP Law by explicitly articulating that confidentiality, integrity, and availability are the fundamental pillars of data security and need to be notified if breached.

(2) The DP Law mandates excessive notification/communication requirements

The GPDR has established its data protection rules and mechanisms based on 'risk'. It is noteworthy that the term 'risk' is articulated seventy-five times throughout the GDPR, including recitals. The Directive 95/46/EC also articulates the term 'risk' throughout eight instances. Under the EU law, the breach notification system is built-up on the risk. The DP Law, on the other hand, does not articulate the term 'risk' within its main text.

Although the GDPR introduces the obligation to notify a breach, it has various exemptions. To recap, notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals whereas communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

Under the GDPR, while every risk requires notification of the breach to the supervisory authority, only high risk necessitates communication to the data subjects. However, under the Turkish Law, though, there is not much distinction or exemption. Data controllers are obliged to notify the DP Board and communicate the breach to the data subjects regardless of the nature or scope of the breach.

When it comes to data breach notification the GDPR builds a rational system. As discussed, under the GDPR, the data controller is exempted from communication if technical, risk-based, or practical grounds justify it. The DP Law, though, does not provide any such exemption.

It is noteworthy that there is a prevailing public interest in disclosing threat. A wise public policy, in this regard, must be the prevention of the problem in the first place. The key policy priority should therefore be to invest in the long-term care of cyber resilience and incentivise the notification of breaches accordingly. The DP Law, though, does not provide any such exemptions for the data controllers.

The obligation to communicate the breach in all cases regardless of the nature and scope of the breach imposes a significant burden on the data controllers. Such burdensome requirements could create psychological barriers to the notification of data breaches. The lack of objective criteria for communication of personal data breach to the data subjects a shortcoming of the Turkish law. The current legal framework and practise fail to protect the data subjects from unnecessary notification fatigue. There is a need to reform the law and limit the instances of notification and communication.[123]

123 For a similar criticism see Çekin (n 112) 112.

(3) The risk of public exposure due to excessive requirements of notification creates a psychological barrier

Due to the requirement to notify and communicate all breach scenarios regardless of the risk, data controllers also bear the risk of being publicised through the publication of the breach on the DP Authority's website. To recap, it could be said that the publication of such a breach is the most drastic sanction of a data breach. These outcomes could create a psychological barrier to the notification of breaches. The motivation to avoid such a public appearance could lead the data controllers to refrain from notification of a breach.

The publication of breaches stigmatises the data controller. Over time, policymakers might consider an institutional "*right to be forgotten*" where entities can legally remove data breach news from online sources.

(4) The time limit of 72-hour notification is too short considering the burden of notification and communication

Almost all data breach incidents need to be reported to the DP Board and communicated to the data subjects. The time limit for the notifications to relevant authorities is 72 hours whereas the very same breach needs to be communicated to data subjects in the shortest reasonable time. The lack of exceptions or exemptions of notification and communication increases the burden of the data controllers.

In this context, late notification is inevitable. However, the late notification or communication is also sanctioned by the DP Board. Considering the consequences of notification such as administrative fines being publicly exposed, the data controllers could refrain from notifying the DP Board. The low numbers of notifications prove the fact that data controllers refrain from a notification.

(5) The ex-officio expansion of investigations to matters not directly related to data breaches give rise to institutional reluctance while notifying a breach

When a data controller notifies a data breach, the DP Board can also expands its investigation into other compliance pillars of the DP Law. For instance, a data controller notifying the DP Board of a security incident related to certain local computers could face a further investigation questioning the international data transfer policy of such company which is not directly related to the security event.

Without a doubt, the DP Board can expand the scope of the investigation ex-officio. However, such exercise of the discretion has indirect consequences. As stated above, the rationale behind the regulation of data breach notification is to prevent or mitigate all adverse effects or damage emanating from a data security incident. This

enables the data subjects to take any remedial measures, e.g., changing passwords and cancelling credit cards. The fear of being under broad scrutiny of the DP Board for the subjects not related to the security incident gives rise to institutional reluctance while notifying a breach. The DP Board's legal but strategically questionable action evolves into a catalyst for burying the evidence.

A breach notification not only serves the parties of the incident but also creates an opportunity for all stakeholders within the data processing community to update their systems since it uncovers the unknown security vulnerabilities, problematic processing methods, or persistent threats. In this regard, any unnecessary burden imposed will undermine the public interest. To promote notification by data controllers, the data breach rules and practice needs to be treated separately. This will increase the number of cases reported and henceforth will maximise the public benefit.

(6) The lack of specific provisions for joint-controllers creates legal uncertainty

The DP Law does not regulate joint-controllers. The lack of a specific provision regulating joint controllers adds another burden on the data controller when they act collectively in a specific processing activity.

(7) The lack of clear methodology for calculating administrative fines is a significant shortcoming

The discretion granted to the DP Board is relatively wide. To disperse the clouds of ambiguity and provide legal certainty, there is an actual need for a secondary regulation to be issued by the DP Authority that lays down the methodology of calculation of administrative fines in case of a data breach.

Notification of breach must be incentivised. How the infringement became known to the data protection supervisory authority, in this regard, must be the key factor in determining the fine. If a data collector or a data processor is fulfilling their legal obligations and cooperating with authorities, fines should be mitigated or altogether removed and replaced with a notice of reprimand to encourage responsible behaviour.[124]

Under the current practice, the data collector is asked to fill the standardized data breach notification form and lay down the technical and organizational measures taken by the data controller before and after the breach. The DP Board, while determining the administrative fine to be levied, takes into account measures taken after the occurrence of the security incident as thresholds while determining the necessary security measures.

124 Eventually, the breach notification is an action of self-disclosure. The outcomes of such notification could lead to administrative, civil, and criminal proceedings. It could be argued that this obligation might be intertwine with or even paradoxical to the general principle of law that no one shall be compelled to make a statement that would incriminate himself/herself or to present such incriminating evidence. For instance see Article 38 of the Turkish Constitution.

Indeed, cyber threats against information security are evolving rapidly and threat agents are also diversifying.[125] Agents such as attackers, bot-network operators, criminal groups, foreign intelligence services, insiders, phishers, spammers, spyware/malware authors, terrorists, and industrial spies target entities by using tools at varying sophistication levels. A major vulnerability could remain undetected for years. The level of protection needs to adjust regularly in accordance with the risks to the information security posed by internal and external threats. It is natural to adopt an unusually high-level security measure after an unprecedented attack. Therefore, the measures taken during extraordinary periods should not be taken as the threshold of liability.

Conclusion

Cyber threats against information systems are evolving rapidly and the threat agents are also transforming. Security breaches are regarded as one of the most serious risks and no entity is immune from a security breach.[126] An average term to diagnose and analyse a data breach is predicted to be 280 days.[127] In this context, there is a silent war between entities and attackers. Furthermore, cyber activities have likewise become "*an integral part of international relations*".[128]

Sustaining the most viable security level without hindering the momentum of digitalisation is a truly complicated task. As rightfully pointed out by Sharma:

> "*It is ironic that hackers and other threats to personal data are the driving force of data protection and cyber-security growth. As cyber-security mechanisms become tougher, hacking practices become more intensive. This creates a continuous cycle, where companies are unaware of how vulnerable their data is until the worst scenario occurs.*"[129]

Nevertheless, regulations worldwide drive entities to make major investments to ensure the most viable protection of their information systems.[130] Companies invest into cutting-edge technologies for maintaining information security. For that purpose, artificial intelligence-based tools are being deployed for detecting insider data leaks.

125 CISA, '*Cyber Threat Source Descriptions*' https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions [accessed 1 March 2021].

126 For instance, '*United Nations data breach exposed over 100k UNEP staff records*' https://www.bleepingcomputer.com/news/security/united-nations-data-breach-exposed-over-100k-unep-staff-records/ [accessed 1 March 2021].

127 IBM, '*Cost of a Data Breach Report 2020*' https://www.ibm.com/security/digital-assets/cost-data-breach-report/ [accessed 1 March 2021].

128 The German Federal Government, '*On the Application of International Law in Cyberspace Position Paper*' https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf [accessed 1 March 2021].

129 Sharma (n 81) 94.

130 According to a study, %77 of the entities who have made investment for boosting their cyber security considers the driving factor of such action as regulations. See, TÜSİAD, '*2020 Türkiye Siber Risk Algı Araştırması*' https://tusiad.org/tr/yayinlar/raporlar/item/download/9428_0ff86134737e19b44a7425cb059f44f8 [accessed 1 March 2021] 2.

However, this kind of practices lead to massive employee surveillance. Drawing the boundary between the legitimate interests of data controllers and the privacy of workers and establishing balance is a quite complex task.

A security breach can compel the data controller to notify the breach to the competent supervisory authority and communicate all facts to the data subjects. As discussed, the underlying aim of this obligation is to prevent or mitigate all adverse effects or damage deriving from a data breach incident.

The EU, in this regard, with its pioneer legislation, i.e., the GDPR, comes forward. As explored in-depth, the data protection eco-system constituted by the GDPR stands on six pillars: coherent rules, simplified procedures, coordinated actions, user involvement, more effective information, and stronger enforcement powers.[131] The GDPR creates a balanced breach notification mechanism. Under the EU law, while every risk requires notification of the breach to the supervisory authority, only high risk necessitates communication to the data subjects. There are also certain exemptions and exceptions to these rules.

In the same way, the most prominent innovation of the Convention 108+ is the obligation to uncover data breaches and the requirement to notify, without delay, any security breaches to the competent authorities. The Convention 108+ also narrows the data breach notification to cases that may seriously interfere with the rights and fundamental freedoms of data subjects, which should be notified.

The Turkish DP Law is mostly modelled after the Directive 95/46/EC with substantial inspiration from the GDPR. The legal framework is tailored up in accordance with the Turkish political and social contexts. There are similarities, even identical provisions with the EU law at as much as there are substantial deviations from the acquis. The shortcomings of the DP Law could be summarised as follows:

(1) The DP law fails to address all types of security breaches that requires notification

(2) The DP Law mandates excessive notification/communication requirements

(3) The risk of public exposure due to excessive requirements of notification creates a psychological barrier to reporting

(4) The time limit of 72 hours notification is too short considering the burden of notification and communication

(5) The ex-officio expansion of investigations to matters not directly related to data breaches give rise to institutional reluctance while notifying a breach

131 The WP29 '*Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*' (n 71) 4.

(6) The lack of specific provisions for joint-controllers creates legal uncertainty

(7) The lack of clear methodology for calculating or enforcing administrative fines is a significant shortcoming

Cyber-attacks and threats targeting data processing systems are also targeting the Turkish network and information realm. While Turkey suffers from cyber-attacks, it has a low number of data breach notifications. Based on the statistics and decisions of the DP Board, the present legal framework leads to a situation that could be called as "*notification-phobia*".

While information security incidents take place in Turkey, these data breaches are not reported adequately. The data controllers chose to bury pieces of evidence due to the burdensome design of the legal framework, the fear of being heavily sanctioned, and the risk of being stigmatised due to publication of the incident in all public mediums. The DP Law leads to a dilemma: self-disclosure or burying the evidence.

The Turkish government has the political target of adopting the EU's data protection norms. Having similar rules and practice is beneficial for both Turkey and the EU considering the cross-border nature of the cyber threats and the close social and economic ties between Turkey and the EU accordingly.

The problem that has become increasingly obvious is that strict and burdensome data breach notification rules do not serve the overall protection of data protection of individuals as data controllers could refrain from notification and bury the pieces of evidence. Such notification-phobia is a major threat to the overall cybersecurity realm. There is a need for balanced rules and adequate accountability tools which would encourage data controllers to disclose any data breach incidents without reluctance.

Sharing information will not extinguish cyber threats but will considerably decrease their effect.[132] As discussed earlier, a major vulnerability could remain undetected for years. Knowing the presence of the virus, its origin, variations, and potential effects are fundamental for preventing infection to evolve into a pandemic. There is a prevailing public interest in disclosing threats. A wise public policy, in this regard, must be the prevention of the problem in the first place. Accordingly, the breach notification must be incentivised in order to strengthen Turkey's overall cyber resilience.

132 Centre for Maritime Law, '*Maritime Industry: Cyber-Risk & Security*' https://cmlnluo.law.blog/2020/01/05/maritime-industry-cyber-risk-security/ [accessed 1 March 2021].

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Financial Disclosure: The author declared that this study has received no financial support.

Bibliography

Article 29 Data Protection Working Party, '*Guidelines on Personal data breach notification under Regulation 2016/679 (Adopted on 3 October 2017 As last Revised and Adopted on 6 February2018)*' https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827

Article 29 Data Protection Working Party, '*Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 Adopted on 3 October 2017*' http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

Burdon M, Lane B and Von Nessen P, '*Data breach notification law in the EU and Australia e Where to now?*' (2012) 28 Computer Law & Security Review.

Council of Europe, '*Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*' https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

Çekin, M S, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu* (On İki Levha 2018).

Determann L, *Determann's Field Guide to Data Privacy Law (Fourth Edition)* (Edward Elgar 2020).

DiGrazia K, '*Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach*' (2018) 13 Journal of Business & Technology Law 225.

Dülger, M V, *Kişisel Verilerin Korunması Hukuku 2. Baskı* (Hukuk Akademisi 2019).

EBA, '*Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) EBA/GL/2017/10, 27.07.2017*'. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

EDPB '*Guidelines on Examples regarding Data Breach Notification Adopted on 14 January 2021 Version 1.0*' https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

ENISA, '*Guidelines for Securing the Internet of Things*' (November 2020) https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

ENISA, '*Incentives and barriers of the cyber insurance market in Europe*' https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport

Gogolin G, *Digital Forensics Explained (Second Edition)* (CRC Press 2021).

Gorecki A, *Cyber Breach Response That Actually Works* (Wiley 2020).

Henkoğlu T, *Adli Bilişim - Dijital Delillerin Elde Edilmesi ve Analizi* (Pusula 2014).

Herrmann D and Pridöhl H, '*Basic Concepts and Models of Cybersecurity*' in Christen M, Gordijn B and Loi M (eds), *The Ethics of Cybersecurity* (Springer 2020).

Hert P and Papakonstantinou V, '*The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*' (2014) 30 Computer Law & Security Review 633.

Karayazgan A, *Hukuki Yönüyle Siber Riskin Sigorta ve Reasüransı* (Legal 2020).

Lambert P B, *Understanding the New European Data Protection Rules* (CRC Press - Taylor & Francis 2018).

Mantelero A, Vaciago G, Esposito M S, Monte N, 'The common EU approach to personal data and cybersecurity regulation' (2021) 1 International Journal of Law and Information Technology 1.

Middleton K and Kazamia M, '*Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concerns*' in Marano P, Rokas I and Kochenburger P (eds), *The "Dematerialized" Insurance - Distance Selling and Cyber Risks from an International Perspective* (Springer 2016).

Nicoletti B, *Insurance 4.0: Benefits and Challenges of Digital Transformation* (Palgrave Macmillan 2021).

Porcedda M G, '*Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*' (2018) 34 Computer Law & Security Review 1077.

Sharma S, *Data Privacy and GDPR Handbook* (Wiley 2020).

Wang FF, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (Cambridge University Press 2010).