RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

A COMPARATIVE ANALYSIS OF JOINT DATA CONTROLLERSHIP UNDER EU AND TURKISH LAW*

ÜMİT ÇALIŞKAN**

Abstract

Technological development and the expansion of digital ecosystems have significantly increased the scale, speed and complexity of personal data processing. This evolution has reshaped the legal meaning of "data controller" and brought forward the modern notion of joint data controllership, particularly under the EU's General Data Protection Regulation (GDPR). Although Turkish Personal Data Protection Law No. 6698 (PDPL) does not explicitly regulate joint data controllers, the processing practices of both public and private actors demonstrate that multiple entities frequently determine purposes and means together. Therefore, a comprehensive comparative analysis is necessary to clarify the legal nature, conditions, obligations and liability of joint data controllers under both legal systems. This article consists of three parts. Part I examines the historical evolution of personal data protection, basic concepts such as personal data, sensitive data and data processing, and core principles guiding lawful processing. Part II analyses the emergence, definition and legal basis of joint data controllership, including seminal Court of Justice of the European Union (CJEU) rulings—Wirtschaftsakademie, Jehovah's Witnesses and Fashion ID—which shaped the concept. Part III investigates the consequences of joint data controllership, focusing on liability, compensation, internal allocation of responsibility, and the applicability of joint liability principles in Turkish law. Through this comparative approach, the article demonstrates that Turkey must incorporate explicit joint data controllership rules into the PDPL to close interpretive gaps, strengthen legal certainty, and align its framework with international standards. The analysis also highlights that joint data controllership serves both to enhance data protection and to impose more burdens on organisations operating in complex digital environments.

Keywords: *Personal data, joint data controller, GDPR, PDPL No. 6698, data security, liability.*

---

* This article is based on a part of the author's PhD dissertation titled "Joint Data Controller Under EU and Turkish Law Compared in the Light of Case Law".

** PhD Candidate, Department of European Union Law, Institute of European Studies, Marmara University, Istanbul, Türkiye. caliskanumitla@gmail.com, ORCID: 0009-0004-5073-4173.

How to cite this article/Atıf için: Çalışkan, Ü. (2026). A Comparative Analysis of Joint Data Controllership Under EU and Turkish Law. *Marmara Avrupa Araştırmaları Dergisi*, 34(1), 33-57.

Submission Date: 10.11.2025 **- Acceptance Date:** 30.06.2026

AB VE TÜRK HUKUKUNDA ORTAK VERİ SORUMLULUĞUNUN KARŞILAŞTIRMALI ANALİZİ

Öz

Teknolojik gelişme ve dijital ekosistemlerin genişlemesi, kişisel veri işlemenin ölçeğini, hızını ve karmaşıklığını önemli ölçüde artırmıştır. Bu dönüşüm, "veri sorumlusu" kavramının hukuki anlamını yeniden şekillendirmiş ve özellikle Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) kapsamında modern "ortak veri sorumluluğu" anlayışını ön plana çıkarmıştır. Her ne kadar 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda (KVKK/PDPL) ortak veri sorumlularına ilişkin açık bir düzenleme bulunmasa da, kamu ve özel sektör aktörlerinin işleme uygulamaları, birden fazla kişinin veri işleme amaç ve vasıtalarını birlikte belirlediğini göstermektedir. Bu nedenle, her iki hukuk sisteminde ortak veri sorumluluğunun hukuki niteliğini, şartlarını, yükümlülüklerini ve sorumluluk rejimini açıklığa kavuşturmak üzere kapsamlı bir karşılaştırmalı analiz gereklidir. Bu makale, üç bölümden oluşmaktadır. Birinci bölümde kişisel verilerin korunmasının tarihsel gelişimi, kişisel veri, özel nitelikli kişisel veri ve veri işleme gibi temel kavramlar ile hukuka uygun işlemeyi yönlendiren temel ilkeler incelenmektedir. İkinci bölümde ortak veri sorumluluğunun ortaya çıkışı, tanımı ve hukuki dayanağı; bu kavramı şekillendiren Avrupa Birliği Adalet Divanı'nın (ABAD/CJEU) Wirtschaftsakademie, Jehovah's Witnesses ve Fashion ID gibi emsal kararları ışığında analiz edilmektedir. Üçüncü bölüm ise ortak veri sorumluluğunun sonuçlarına odaklanmakta; sorumluluk, tazminat, iç sorumluluk dağılımı ve Türk hukukunda müşterek sorumluluk ilkelerinin uygulanabilirliği değerlendirilmektedir. Karşılaştırmalı yaklaşım çerçevesinde, Türkiye'nin yorum farklılıklarını gidermek, hukuki öngörülebilirliği güçlendirmek ve uluslararası standartlarla uyum sağlamak amacıyla KVKK'ya ortak veri sorumluluğuna ilişkin açık hükümler eklemesi gerektiği ortaya konulmaktadır. Analiz ayrıca, ortak veri sorumluluğunun hem veri koruma seviyesini yükselttiğini hem de karmaşık dijital ortamlarda faaliyet gösteren kuruluşlara daha fazla yükümlülük getirdiğini göstermektedir.

Anahtar Kelimeler: *Kişisel veri, ortak veri sorumlusu, GDPR, 6698 sayılı KVKK, veri güvenliği, sorumluluk.*

Introduction

The modern digital environment is characterised by complex technological infrastructures, multi-actor ecosystems, cross-platform integrations and decentralised processing architectures[1]. As a result, the protection of personal

[1] Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 2. Baskı, Oxford University Press, 2007, s. 58.

data—once a relatively simple matter of bilateral controller–data subject relations—now frequently involves multiple actors jointly determining the purposes and means of processing[2]. This reality has led to the legal recognition of "joint data controllership," particularly under the GDPR, which explicitly acknowledges that two or more controllers may jointly determine processing operations[3]. Turkish law, by contrast, has yet to explicitly adopt this concept, even though processing operations carried out by public institutions, banks, telecommunications providers, platform-based services and cross-border digital systems frequently involve shared decision-making[4]. In practice, determining "who is the controller" and "who bears liability" becomes increasingly complex, especially when several actors contribute to the architecture of processing[5].

Part I presents the foundations of personal data protection: historical development, basic concepts, types of data, processing principles and the rights of data subjects[6]. Part II focuses on the doctrinal and judicial formation of joint data controllership in EU law, and the implicit reflections of this structure in Turkish legislation[7]. Part III evaluates the nature and consequences of joint controllership, placing emphasis on legal liability, joint and several liability, compensation mechanisms and the relationship between controllers[8]. The article concludes with a critical assessment and comparative findings.

Legal Framework of Personal Data Protection

International Legal Instruments

The contemporary legal regime of personal data protection emerged from the technological, political and institutional transformations following the Industrial Revolution. As automated processing tools proliferated, the value of personal data increased and concerns about misuse led to the first binding international instrument in this field: the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108). Adopted in 1981, Convention 108[9] constituted the foundational step for classifying personal data protection as an autonomous right and required

[2] Lee A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford University Press, 2014, s. 153.
[3] Regulation (EU) 2016/679 (General Data Protection Regulation), m. 26.
[4] Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku*, 3rd ed., Hukuk Akademisi, İstanbul, 2020, p. 182
[5] İrem Kaya, *Kişisel Verilerin Korunması Kanunu ve GDPR Kapsamında Ortak Veri Sorumluluğu*, Master's Thesis, Hacettepe University, 2023, p. 7.
[6] Elif Küzeci *Kişisel Verilerin Korunması*, 5th ed., On İki Levha, İstanbul, 2020, p. 144.
[7] CJEU, Case C-210/16 (*Wirtschaftsakademie*), EU:C:2018:388; Case C-25/17 (*Jehovah's Witnesses*), EU:C:2018:551; Case C-40/17 (*Fashion ID*), EU:C:2019:629.
[8] Regulation (EU) 2016/679 (GDPR), m. 82.
[9] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No 108, 1981), accessed 12 May 2024.

national legal frameworks to regulate automated data processing. Its modernised version, Convention 108+, adopted in 2018[10], strengthened obligations by incorporating transparency requirements, breach notifications, special categories of data, and the principles of privacy by design and privacy by default.

EU Legal Framework

Another milestone was the Directive 95/46/EC[11], which framed data protection as a fundamental right across EU Member States and enabled free data movement within the EU. It introduced core concepts such as lawful processing, correction of inaccurate data and conditions for processing special categories of data. The development of EU data protection law has also been widely discussed in academic literature, particularly in relation to its evolution as a fundamental right and its added value within the EU legal order[12].

Over time, however, divergent national practices created fragmentation between Member States[13]. Rapid technological change—platform economies, cross-border transfers, cloud computing and advanced profiling techniques—made the Directive insufficient[14]. This led to the adoption of the General Data Protection Regulation (GDPR) in 2016, applicable since May 2018. The GDPR harmonised the legal framework through a single regulation, strengthened enforcement via increased administrative fines, introduced new rights (data portability, right to be forgotten), expanded territorial scope and explicitly regulated joint data controllership, recognising the reality of multi-actor processing relationships[15].

Turkish Legal Framework

Personal data protection in Turkey developed later than in Europe. Prior to specific legislative regulation, the Turkish Penal Code (TPC) Articles 135–138[16] criminalised unlawful recording, transfer and failure to delete personal data, but

[10] Council of Europe, *Protocol Amending Convention No 108 (Convention 108+)* (CETS No 223, 2018).
[11] Directive 95/46/EC [1995] OJ L281/31.
[12] Orla Lynskey, "Deconstructing Data Protection", (2014) 63 *International and Comparative Law Quarterly*, p. 569.
[13] Bart Custers – Raphaël Gellert, "Data Protection as a Fundamental Right", (2012) 28(3) *Computer Law & Security Review*, pp. 285–294.
[14] Paul Voigt – Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017.
[15] Christina Kunshier, "The Global Reach of the GDPR", (2018) 40(1) *Michigan Journal of International Law*.
[16] Turkish Penal Code (Law No 5237), Official Gazette, 12 October 2004, No 25611, Arts. 135–138 [in Turkish].

did not define the concept itself[17]. A significant constitutional step came in 2010, when personal data protection was recognised as a constitutional right through an amendment to Article 20 of the Constitution[18], granting individuals the right to be informed, to access, to correct and to request the deletion of personal data. It also required that personal data be processed only with explicit consent or in cases prescribed by law.

Despite early initiatives—such as the 1981 signature of Convention 108 and the drafting attempts of 1995 and 2003—Turkey adopted a comprehensive data protection law only in 2016. The Personal Data Protection Law No. 6698 (PDPL) was enacted on 24 March 2016 and published on 7 April 2016[19]. Although based on Directive 95/46/EC, it partially resembles the GDPR. Article 1 of PDPL aims to protect fundamental rights, especially privacy, in the processing of personal data and to regulate the obligations of natural and legal persons processing personal data. Article 2 defines the scope, covering personal data processed wholly or partially by automated means or by non-automated means forming part of a data recording system[20]. Like GDPR, PDPL applies only to natural persons' data. It excludes certain processing activities such as those conducted for personal use, for artistic or academic purposes, national security, or judicial functions (Article 28)[21].

Basic Concepts

Definition of Personal Data

International and national legal instruments broadly define personal data as "any information relating to an identified or identifiable natural person[22]." This includes not only direct identifiers—name, address, identification number—but

[17] Law No 6669, Official Gazette, 18 February 2016, No 29628 [in Turkish].The "Crimes" section of Article 17 of the Personal Data Protection Law, which came into effect in 2016, establishes a connection between this law and the relevant provisions of the Turkish Penal Code. This relationship emphasizes the importance of data protection in the context of criminal law.

[18] The Law No. 5982 on Amendments to Certain Articles of the Constitution of the Republic of Turkey was published in the Official Gazette (S.27580) on May 13, 2010. This law made significant changes to various provisions of the Turkish Constitution, impacting areas such as individual rights and freedoms, the judiciary, and the political system.

[19] Law No 6669 on the Approval of Convention 108, Official Gazette, 18 February 2016, No 29628 [in Turkish].

[20] Law No 6698 on the Protection of Personal Data (PDPL), Official Gazette No 29677, 7 April 2016, arts 1–2.

[21] İrem Kaya, *Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Ortak Veri Sorumluluğu*, Master's Thesis, Hacettepe University, Ankara, 2023, p. 7 [in Turkish].

[22] Elif Küzeci, *Kişisel Verilerin Korunması*, 3rd ed., Turhan Kitabevi, Ankara, 2021, p. 102 [in Turkish].

also indirect identifiers such as IP addresses, e-mail addresses, professional information, behavioural data and biometric identifiers[23].

In Turkish law, PDPL adopts this broad definition, emphasising identifiability[24]. The Regulation on the Processing of Personal Data in Electronic Communications initially included legal persons, but PDPL corrected this by limiting protection to natural persons[25]. Many authors criticise the open-ended nature of the definition, yet its flexibility ensures adaptability to technological change[26].

Sensitive Data

Sensitive or special categories of data receive heightened protection due to their potential to cause discrimination[27]. Under Directive 95/46 and Convention 108, sensitive data includes race, ethnic origin, political opinions, religious or philosophical beliefs, health, and sexual life[28]. GDPR expands this to include biometric and genetic data and sexual orientation[29]. PDPL Article 6 defines a closed list: race, ethnic origin, political opinion, philosophical belief, religion, sect, appearance, membership of associations/foundations/unions, health, sexual life, criminal convictions and security measures, biometric and genetic data[30]. Only these are considered sensitive. The risk of discrimination—especially regarding religion or health data—explains the strictness of these rules. Abuse may lead to severe violations of privacy, dignity and equality[31].

Processing of Personal Data

GDPR Article 4 defines processing broadly to include all operations performed on personal data: collection, recording, storage, alteration, retrieval, disclosure, combination, restriction, deletion and destruction, whether automated

[23] Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku*, 2nd ed., Hukuk Akademisi, İstanbul, 2020, p. 75 [in Turkish]; European Data Protection Board (EDPB), *Opinion 4/2007 on the Concept of Personal Data*, 2007, pp. 12–14.
[24] Hayrunnisa Özdemir, *Kişisel Verilerin Korunması Kanunu Şerhi*, Yetkin Yayınları, Ankara, 2021, p. 44 [in Turkish].
[25] Ali Rıza Süzek, "Kişisel Veri Kavramı", (2018) 22(4) *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, p. 115 [in Turkish].
[26] Çiğdem Kırca, "Kişisel Verilerin Korunması", *Terazi Hukuk Dergisi*, No. 119, 2016, p. 22 [in Turkish].
[27] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 312.
[28] Küzeci, *Kişisel Verilerin Korunması*, p. 188.
[29] Bygrave, *Data Privacy Law*, p. 68.
[30] Mesut Serdar Çekin, *Kişisel Verilerin Korunması Hukuku*, 2nd ed., On İki Levha Yayıncılık, İstanbul, 2022, p. 145 [in Turkish].
[31] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 61; Ayşe Gönül KILIÇ, "Kişisel Veri Kavramının Belirlenmesine İlişkin Kriterler ve Bir Alt Kategori Olarak Özel Nitelikli Kişisel Veriler", (2019) 25(2) *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, p. 892 [in Turkish].

or not[32].Convention 108 defines automated processing similarly[33]. PDPL's definition mirrors these concepts, requiring that non-automated processing fall within a data recording system[34]. Automatic processing includes any operation done through information systems, where human involvement is limited. PDPL treats automated and manual processing equally if the latter is part of a systematic recording structure[35]. Legislators deliberately avoid limiting the definition with an exhaustive list, due to rapid technological evolution[36].

Basic Principles in the Processing of Personal Data

Core principles are central to determining lawfulness and guiding all stages of data processing—from collection to deletion. They serve as interpretative tools for supervisory authorities when assessing violations. Although various instruments regulate them differently, there is broad consensus across jurisdictions[37]. Within this framework, the need of lawfulness requires processing to comply with statutory provisions and universal legal principles. For example, GDPR Article 6 specifies lawful bases for processing, and Article 5 requires fairness and transparency[38]. Honesty (good faith) requires data controllers to act in accordance with Article 2 of the Turkish Civil Code, which embodies objective good faith standard[39]s. This means acting transparently, respecting expectations, and avoiding deceit or misuse of data[40].

Accordingly, processing incompatible with the reasonable expectations of the data subject violates this principle. Examples include collecting unnecessary sensitive data or misusing customer information for unsolicited advertising. Transparency is a core component under GDPR, requiring accessible and clear processing information[41]. In addition, controllers must determine the purpose of processing explicitly at the time of collection. The purpose must be legitimate and understandable to the data subject. Using data for a purpose unknown to the data subject violates this principle[42].If processing purposes change, renewed

[32] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 125.
[33] Küzeci, *Kişisel Verilerin Korunması*, p. 154.
[34] Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 98.
[35] Özdemir, *Kişisel Verilerin Korunması Kanunu Şerhi*, p. 62.
[36] Süzek, "Kişisel Veri Kavramı", p. 128.
[37]Küzeci, *Kişisel Verilerin Korunması*, p. 144; DÜLGER, *Kişisel Verilerin Korunması Hukuku*, p. 182.
[38] Küzeci, *Kişisel Verilerin Korunması*, p. 215.
[39] Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 112..
[40] Özdemir, *Kişisel Verilerin Korunması Kanunu Şerhi*, p. 88; Hasan Ayrancı – Ahmet Çolak – Onur Özcan, *Kişisel Verilerin Korunması Kanunu Şerhi*, Yetkin Yayınları, Ankara, 2022, pp. 154-156.
[41] Bygrave, *Data Privacy Law*, pp. 153, 155; DÜLGER, *Kişisel Verilerin Korunması Hukuku*, p. 185.
[42] Kuner, *European Data Protection Law*, p. 58.

consent or a new legal basis is needed unless the new purpose is compatible with the original one[43]. GDPR Article 5(1)(b) expressly incorporates purpose limitation; PDPL includes similar provisions.

Likewise, this principle mandates data minimisation: obtaining only what is necessary. Collecting future-use data "just in case" violates proportionality. Controllers must balance the amount of data collected with the intended purpose[44].Retention policies are crucial to implementing this principle. Data collected for one purpose—such as health data for employment suitability—cannot be used for unrelated purposes[45]. GDPR Article 5(1)(c) focuses on data minimisation; PDPL Article 4 mirrors this requirement[46].

Moreover, accuracy ensures that individuals are not harmed by outdated or incorrect data. Controllers have an ongoing obligation to maintain accuracy, especially when decisions affecting the data subject depend on the information (e.g., credit scoring)[47].Data subjects must have means to request correction. Inaccurate information, such as an outdated phone number or address, may cause harm—missed notifications, financial losses, or legal complications[48]. Data must not be stored longer than necessary. Once the statutory or purpose-based retention period expires, the controller must delete, destroy or anonymise the data. Retention beyond necessary limits increases risk of breaches and loss of control. PDPL Article 7 regulates deletion, destruction and anonymisation, requiring controllers to act ex officio or upon request[49].

Furthermore, data subjects hold essential rights enabling them to control personal data and activate legal mechanisms. These rights exist without a need for prior contact with the controller. Controllers must inform data subjects about processing purposes, legal bases, storage, transfers and rights. Transparency enables autonomous decision-making[50]. Under GDPR, this appears as the right

[43] Küzeci, *Kişisel Verilerin Korunması*, p. 218.
[44] Çiğdem Ayözger, *Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, 2nd ed., Beta Basım Yayın, İstanbul, 2019, p. 138 [in Turkish]; Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 115.
[45] Stewart Room, *Data Protection & Compliance in Context*, The British Computer Society, United Kingdom, 2007, p. 106.
[46] Özdemir, *Kişisel Verilerin Korunması Kanunu Şerhi*, p. 92.
[47] Küzeci, *Kişisel Verilerin Korunması*, p. 220.
[48] Ayrancı – Çolak – Özcan, *Kişisel Verilerin Korunması Kanunu Şerhi*, p. 162.
[49]Law No 6698 on the Protection of Personal Data, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, accessed 12 May 2024 [in Turkish]; Şahin Ardıç, "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi", (2018) 24(2) *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, p. 748 [in Turkish].
[50] Küzeci *Kişisel Verilerin Korunması*, p. 225.

to transparent information. Under PDPL, it is formulated as a disclosure obligation[51].

In this context, individuals must have the ability to access data held about them, along with information on processing purposes, recipients and retention. Access enables verification of accuracy and lawfulness. This right also supports the right to rectify, block or delete data. Under GDPR, access is comprehensive; PDPL enumerates specific information that may be requested. PDPL Article 7 regulates destruction processes triggered by expiration of purpose, expiry of legal basis, withdrawal of consent or unlawful processing[52]. Deletion removes accessibility; destruction physically eliminates stored data; anonymisation renders identification impossible even by matching with other datasets. Controllers must act proactively, even without data subject request[53].

Finally, the digital age has made perpetual memory a dangerous reality for privacy and rehabilitation. The right to be forgotten aims to prevent disproportionate harm from outdated or irrelevant information[54].The CJEU's Google Spain ruling established that search engines qualify as data controllers and must remove links under certain circumstances[55]. Criteria include relevance, accuracy, sensitivity, passage of time and the role of the individual in public life[56].

To sum up, Turkish Constitutional Court acknowledged the right to be forgotten in N.B.B. (2013/5653), grounding it on Articles 5, 17 and 20 of the Constitution. It established balancing tests and criteria for evaluating requests. The Court of Cassation later applied these principles in defamation and privacy cases. The Turkish Data Protection Board's 2020/481 decision further operationalised the right regarding search engines[57]. GDPR Article 20 introduced this right, enabling individuals to obtain personal data in a machine-readable

[51] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 442.
[52] Ayözger, *Kişisel Verilerin Korunması Hukuku*, p. 46; ÖZDEMİR, *Kişisel Verilerin Korunması Kanunu Şerhi*, p. 165.
[53] Ardıç, "Kişisel Verilerin Silinmesi…", p. 752.
[54] İrem Laçin, "Unutulma Hakkı", *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, 2014, p. 112, http://dosya.gsu.edu.tr/Docs/HukukFakultesi/TR/FakulteDergisi/GUHFD_2014_1.pdf [in Turkish].
[55] Küzeci*Kişisel Verilerin Korunması*, p. 310.
[56] Cécile De Terwangne, "The Right to be Forgotten and the Informational Autonomy in the Digital Environment", http://publications.jrc.ec.europa.eu/repository/bitstream/JRC86750/jrc86750_cecile_fv.pdf, p. 2, accessed 12 May 2024; Kuner – Bygrave – Docksey, *GDPR Commentary*, p. 445.
[57] Murat Volkan DÜLGER, "Unutulma Hakkı: Dijital Hafızadan Silinmeyi İstemek", *Terazi Hukuk Dergisi*, No. 120, 2016, p. 48 [in Turkish].

format and transfer it between controllers. It enhances user autonomy and market competition[58].PDPL does not include a similar explicit right[59].

Joint Data Controllership

Legal Framework

The emergence of joint data controllership is closely linked to the increasing complexity of modern data ecosystems. Under the traditional model, data protection frameworks assumed a simple bilateral relationship: one controller determines the purposes and means of processing, and one processor executes those instructions[60]. The digital environment, however, routinely involves multiple actors who jointly shape processing activities—social media platforms and advertisers, political organisations and volunteers, website owners and analytics providers, banks and fintech partners, platform operators and merchants, and public authorities sharing interconnected databases[61].

The GDPR responded to this reality by explicitly recognising that "two or more controllers" may "jointly determine the purposes and means of the processing" (GDPR Art. 26). This marked a structural departure from Directive 95/46/EC, which implied but never openly regulated joint controllership[62]. The GDPR not only acknowledged this model but imposed obligations on joint controllers to transparently allocate responsibilities, provide data subjects with clear information, and ensure compliance regardless of internal arrangements[63].

In this context,while the PDPL does not explicitly mention joint controllers, its definition of "data controller" does not exclude scenarios where multiple actors determine purposes and means together[64]. The functional approach of PDPL, focusing on actual decision-making rather than formal labels, enables the concept to be inferred doctrinally. However, the absence of explicit provisions

---

[58] EUR-LEX, Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679, accessed 20 April 2022.

[59] Özge Evre, "Veri Taşınabilirliği Hakkı ve Türk Hukuku Bakımından Değerlendirilmesi", (2021) 79(1) *İstanbul Hukuk Mecmuası*, p. 140 [in Turkish].

[60] Yordanka Ivanova, "Data Controller, Processor or a Joint Controller…", in: Maria Tzanou (ed.), *Personal Data Protection and Legal Developments in the European Union*, 2020.

[61] European Data Protection Board (EDPB), *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR*, 2021, https://edpb.europa.eu/..., 12 May 2024; Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 242.

[62] Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020), 578.

[63] Millard – Kamarinou, "Article 26: Joint Controllers", in: Kuner – Bygrave – Docksey (eds.), *GDPR Commentary*, Oxford University Press, 2020, p. 584; Küzeci *Kişisel Verilerin Korunması*, p. 265.

[64] Çekin *Kişisel Verilerin Korunması Hukuku*, p. 168.

leads to ambiguity regarding liability allocation, notification duties, and the relationship between multiple controllers[65].

Judicial Development of Joint Controllership

Key CJEU Decisions

Three landmark CJEU cases—Wirtschaftsakademie Schleswig-Holstein (2018), Jehovah's Witnesses (2018), and Fashion ID (2019)—form the jurisprudential backbone of joint controllership in EU law. Each decision expanded the criteria for identifying joint controllers by emphasising functional influence over purposes and means rather than formal agreements[66].

Wirtschaftsakademie Schleswig-Holstein (C-210/16)

This case involved an educational company administering a Facebook fan page. The Schleswig-Holstein Data Protection Authority required the company to deactivate the page due to Facebook's inability to meet data protection requirements. The company contested, arguing that Facebook, not the page administrator, processed personal data. The CJEU held: Both Facebook and the page administrator were joint controllers.[67]

In particular, the administrator influenced processing by determining audience parameters, visitor statistics and marketing objectives. The definition of "controller" must be interpreted broadly to ensure effective protection. The Court stressed that joint controllership does not require equal responsibility or equal involvement; even partial influence over certain stages of processing may suffice[68].

Jehovah's Witnesses (C-25/17)

The case concerned door-to-door preaching by members of the Jehovah's Witnesses religious community. Members collected personal data (names, addresses, beliefs) during visits. The question was whether the community could be considered a controller alongside individual preachers. Similiarly, The CJEU held that: A religious community is a joint controller when it organises and coordinates preaching activities[69].

---

[65] Kadem, "Ortak Veri Sorumlusu Kavramı…", *MÜHFAD*, 2020, pp. 1012–1015

[66] Dülger, "GDPR'da Bulunan Ancak KVKK'da Yer Verilmeyen Bir Kavram…", 2021, p. 2, https://www.academia.edu/...,12 May 2024; Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 248.

[67]CJEU, Case C-210/16, *Wirtschaftsakademie*, https://curia.europa.eu, accessed 12 May 2024; Kuner – Bygrave – Docksey, *GDPR Commentary*, p. 582.

[68] Küzeci, *Kişisel Verilerin Korunması*, pp. 268–270.

[69]Court of Justice of the European Union (CJEU), C-25/17, Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta,

The community encouraged data collection and maintained centralised records, influencing both purposes and means. Processing need not be carried out jointly; joint determination of objectives is sufficient. The decision broadened the concept further: organisational support or encouragement may create joint controllership even without technical control of data[70].

Fashion ID (C-40/17)

This case addressed the embedding of a Facebook "Like" plug-in on a fashion retailer's website. The plug-in automatically transmitted user data (IP address, browser data) to Facebook when visitors accessed the website. Furthermore, The CJEU held: The website operator and Facebook were joint controllers for the data collection and transmission triggered by the plug-in[71].

The operator determined that data would be collected and transmitted by choosing to embed the plug-in for marketing advantage. However, the operator was not a controller for subsequent processing performed independently by Facebook.This case established the principle of partial joint controllership: an entity may be a joint controller only for certain stages of processing, not for the entire lifecycle[72].

Formation of Joint Data Controllership

Definition and Conditions

Joint data controllership arises when two or more actors jointly determine the purposes and means of processing. Determination of purposes refers to deciding "why" data is processed; determination of means concerns the "how"—tools, methods, infrastructure and organisational decisions[73]. EU case law and EDPB guidance emphasise functional analysis: Who genuinely influences or determines the essential elements of processing?[74]

Accordingly, joint controllership exists when: Two or more parties participate in determining purposes. Each party has a degree of practical influence, even if

https://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=EN (a.d. May,12,2024; Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 172; Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1025.

[70] Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1025

[71]CJEU, Case C-40/17, *Fashion ID*, https://curia.europa.eu, accessed 12 May 2024; Ayşe Gönül Kılıç, "Avrupa Birliği Adalet Divanı Kararları Işığında Ortak Veri Sorumluluğu", *Hukuk Köprüsü*, No. 18, 2020, pp. 42–45 [in Turkish].

[72] Elif Küzeci – Şebnem Kılıç, "6698 Sayılı KVKK'nın İş Sözleşmesi Çerçevesinde Değerlendirilmesi…", (2019) 16(63) *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi*, p. 960 [in Turkish]; Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 255.

[73] Welfare – Carey, p. 18; Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 258.

[74] EDPB, Guidelines 07/2020, para. 48.; European Data Protection Board (EDPB), *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR* (2021), 18–21.

not equal. The determination results from a common decision or converging decisions that complement each other. Processing would not occur without the combined participation of both parties[75].

Indicators of Joint Controllership

Indicators include: Joint planning of processing operations. Shared databases or information systems. Mutual benefit from processing. Coordinated communication or notification procedures. Embedding third-party tools (e.g., plug-ins, cookies)[76].

Legal Obligations of Joint Controllers

Under GDPR Art. 26(1), joint controllers must define their responsibilities transparently via an arrangement, specifying: the handling of data subject rights, the provision of information to data subjects, the allocation of compliance obligations[77]. Responsibility is allocated internally but does not affect data subjects, who may exercise their rights against any controller[78]. In this respect, under Turkish law, PDPL lacks a corresponding provision. Nevertheless, a functional interpretation of Articles 3 and 4 indicates that entities jointly determining purposes and means may be treated as controllers concurrently[79]. However, without explicit rules, ambiguity persists regarding notification responsibilities, liability sharing and the coordination of responses to data subject requests[80].

Determination of Purposes and Means

Joint determination of purposes and means does not require equal participation. As clarified in Fashion ID, even partial influence over criteria essential to processing—such as choice of plug-ins or structured data collection—is sufficient[81]. Purposes may include: marketing and advertising strategies, security operations, risk assessments, fraud prevention, public service provision, organizational coordination. As a result, means may include: selection of IT systems, determination of data categories, decision to deploy analytics tools, retention protocols, technical or organizational features. Importantly, in many modern scenarios, determination occurs implicitly[82]. A company using social media tracking pixels jointly determines data collection parameters with the platform provider. Banks sharing customer scoring data with fintech partners

[75] Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1028.
[76] Küzeci, *Kişisel Verilerin Korunması*, p. 272.
[77]EDPB, Guidelines 07/2020, para. 57.
[78] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 262.
[79] Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1035..
[80] Kılıç, "Ortak Veri Sorumluluğu", p. 52.
[81] Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 175.
[82] EDPB, *Guidelines 07/2020*, para. 168; Küzeci *Kişisel Verilerin Korunması*, p. 278.

jointly determine the criteria for credit assessment. Public authorities operating integrated databases jointly shape the architecture of processing[83].

Practical Examples and Sectoral Applications

Under PDPL, although the concept is not codified, similar situations arise frequently. For example: Hospitals and laboratories jointly determining diagnostic data flows. E-government platforms integrating services of multiple ministries. Logistics companies and e-commerce platforms using shared databases[84]. Turkish scholars argue that joint controllership must be recognised doctrinally to address these realities in sectors such as healthcare, finance, telecommunications and e-commerce[85].

Obligations of Joint Data Controllers

Joint controllers bear obligations similar to sole controllers but must coordinate their responsibilities. Under GDPR Art. 26, joint controllers must reach an arrangement determining their respective roles. This arrangement must reflect the real influence of each controller over processing activities.[86] Ensuring lawful processing (legal bases, legitimate purposes), implementing transparency measures (clear and accessible privacy notices), allocating responsibility for responding to data subject rights, data security obligations (technical and organisational measures), notification of data breaches to authorities and affected individuals and maintaining documentation (records of processing activities) can be regarded as key obligations[87].

Allocation of Responsibilities Between Joint Controllers

The sharing of obligations should reflect: Functional control – Each controller's real influence over purposes and means. Operational capacity – Entities with greater technical or administrative capacity often handle security and compliance tasks. Therefore, Risk distribution – Controllers allocate responsibilities to mitigate collective risks[88].

---

[83] Selin Çetin, "Veri Sorumlusu ve Veri İşleyen…", (2020) 2(1) *Bilişim Hukuku Dergisi*, pp. 15–18 [in Turkish].
[84] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 265.
[85] Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1040.
[86] Mahieu, Rene/ Hoboken, van Joris, "Fashion-ID: Introducing a Phase-Oriented Approach to DataProtection?", European Law Blog, 2019, para.12. https://europeanlawblog.eu/2019/09/30/fashionid-introducing-a-phase-oriented-approach-to-data-protection/ a.d.May,12,2024; KÜZECİ, *Kişisel Verilerin Korunması*, p. 282.
[87] Çekin *Kişisel Verilerin Korunması Hukuku*, p. 180; Çetin, "Veri Sorumlusu…", p. 22..
[88] Valentina Colcelli, "Joint Controller Agreement under GDPR", (2019) *EU and Comparative Law Issues and Challenges Series*, pp. 1030–1047; Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 270.

Under GDPR, internal arrangements may allocate responsibilities; however, data subjects may exercise their rights against any controller, preserving their protection[89]. Under PDPL, ambiguous provisions complicate responsibility-sharing. Since the law does not regulate joint controllership, questions arise: Must all controllers separately fulfill notification duties? Who responds to data subject requests? Who conducts deletion, destruction or anonymization? How is liability distributed? The lack of explicit provisions creates practical challenges for organizations and leads to inconsistent practices across sectors[90].

Arrangement Between Joint Controllers

GDPR Art. 26 [91]requires a binding arrangement, often in the form of: Contractual agreements, Joint governance frameworks, Standardized collaborative templates. Such arrangements typically specify: Responsibilities for disclosure obligations, Contact points for data subjects, Mechanisms for cooperation, Security measures and incident handling, Retention periods, Data sharing protocols[92]. In practice, even if not fully formalized, controllers must be able to demonstrate compliance[93]. DPPL does not impose such an arrangement requirement. As a result, informal or tacit processing relationships—common in Turkey—may occur without clear governance structures, increasing the risk of accountability gaps[94].

Liability and Compensation

Liability under GDPR

Under GDPR Art. 82: All controllers involved in processing may be held jointly and severally liable for damages[95]. A controller that pays full compensation may seek contribution from others depending on their share of responsibility[96]. CJEU case law reinforces this broad principle of liability: individuals must not be deprived of effective redress[97].

---

[89] Valentina Colcelli, "Joint Controller Agreement under GDPR", (2019) *EU and Comparative Law Issues and Challenges Series*, No. 3, pp. 1030–1047, at 1040.
[90] Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1045.
[91] Burkhard HESS, *The Unclaimed Territory of the GDPR: Joint Controllership and Liability*, pp. 2, 11. ; Duc Tran – Laura Adde, "Joint Controller Relationships: More Prevalent Than Previously Thought?", (2019) 19(8) *Privacy & Data Protection*, pp. 6–8, at 6.
[92] Küzeci, *Kişisel Verilerin Korunması*, p. 285.
[93] Alsenoy, *Data Protection*, p. 74; Millard – Kamarinou, p. 583..
[94] Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 185.
[95] Jenai Nissim, "Accountability and the Role of the Data Protection Officer", in: Peter Carey (ed.), *Data Protection*, Oxford University Press, Oxford, 2018.
[96] Brendan Alsenoy, "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", (2016) 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, pp. 271–288, at 279.
[97] Kuner – Bygrave – Docksey, *GDPR Commentary*, pp. 1142–1145.

Liability under Turkish Law

Under PDPL Art. 11 and Art. 14, data subjects may claim compensation for material and moral damages. Liability arises from unlawful processing, failure to ensure data security, or breach of obligations. The law does not specify whether multiple controllers may be jointly liable[98]. This uncertainty strengthens the argument for legislative reform to incorporate joint controllership provisions to ensure predictable and fair liability structures[99].

Nature And Consequences Of Joint Data Responsibility

Legal Liability of Joint Data Controllers Under GDPR

Under the GDPR, liability is constructed to ensure effective protection of data subjects in multi-actor processing situations[100]. Article 82 sets out a comprehensive and protective liability regime, establishing that any controller involved in processing may be held liable for the entirety of the damage, regardless of their internal allocation of responsibilities. This serves two central goals: Guaranteeing complete compensation for the data subject. Ensuring accountability for controllers who participate in or benefit from the processing[101]. The GDPR adopts two interrelated concepts: Joint and several liability of controllers; Right of recourse between controllers internally[102].

In this content, even if a particular controller is responsible only for a segment of the processing operation, they may still be sued for full compensation. This broad and protective interpretation is consistent with the CJEU's functional approach in Fashion ID, Wirtschaftsakademie, and Jehovah's Witnesses: once an entity jointly determines the purposes or essential means, even minimally, it becomes responsible for compliance in relation to that stage of processing[103]. In addition, the GDPR requires controllers to demonstrate compliance ("accountability principle," Art. 5(2)). Documentation of responsibilities, adequate security measures, transparent communication with data subjects, and cooperation with supervisory authorities are all part of this obligation[104]. Importantly, internal contractual arrangements between joint controllers cannot

[98] Çetin, "Veri Sorumlusu…", p. 25.
[99] Ayşe Gönül Kılıç, "Avrupa Birliği Adalet Divanı Kararları Işığında Ortak Veri Sorumluluğu," *Hukuk Köprüsü*, no. 18 (2020): 55–58.
[100] A. B. Menezes Cordeiro, "Civil Liability for Processing of Personal Data in the GDPR", (2019) 5(4) *European Data Protection Law Review*, pp. 492–499, at 492.
[101] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 275.
[102] Kuner – Bygrave – Docksey, *GDPR Commentary*, p. 1150.
[103] Jonas Knetsch, "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases", (2022) 13(2) *Journal of European Tort Law*, p. 138; KILIÇ, p. 58.
[104] Knetsch, p. 148; Küzeci, *Kişisel Verilerin Korunması*, p. 288.

reduce liability toward the data subject. No contractual clause can waive the rights granted to individuals under GDPR Art. 82[105].

Common Data Responsibility Under the Scope of the Turkish Personal Data Protection Law

The PDPL does not explicitly address joint data controllership. This omission creates interpretive challenges, because the law assumes a model in which each processing activity has a singular controller. However, Turkish practice in public administration, finance, health, e-government systems, and private sector digital services shows that processing activities often involve multiple controllers. Despite the absence of explicit regulation, PDPL's functional definition of "data controller" ("the natural or legal person who determines the purposes and means of data processing") indicates that more than one entity may simultaneously fulfil this role[106].

Therefore, Turkish scholarship argues that joint controllership exists de facto in many situations, including: integrated public data systems (e-Devlet, MERNİS); sector-wide shared databases (credit reference systems); collaborative data processing between hospitals and laboratories; e-commerce platforms and logistics providers jointly determining data flows[107]. Yet because PDPL has no Article comparable to GDPR Art. 26, there is: no explicit requirement for a joint arrangement; no formal allocation of responsibilities; unresolved questions on liability distribution; ambiguity concerning disclosure obligations and data subject request handling[108]. This leads to fragmented interpretations by controllers, regulatory uncertainty, and inconsistent enforcement.

Legal Liability of Data Controllers and Joint Data Controllers

Under PDPL, liability is based on: unlawful processing (Art. 12); failure to ensure data security; failure to delete/anonymise data (Art. 7); failure to fulfil disclosure or registry obligations. The law provides for both administrative sanctions and compensation for damages (Art. 11, 14, 15). However, it does not explicitly state whether liability is joint, several, or joint and several when multiple controllers share responsibility.

In practice, the following questions arise: If two controllers jointly determine the purposes of processing, are they liable equally? Does the data subject have the right to sue either controller for full compensation? Can a controller seek

[105] Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 192.
[106] Dülger, "Ortak Veri Sorumluluğu", p. 2.
[107] Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1042.
[108] Çekin, *Kişisel Verilerin Korunması Hukuku*, p. 195.

recourse against others proportionate to their *c*ontribution? Does failure by one controller to fulfil disclosure obligations affect the liability of the other?

Actually, Turkish courts sometimes apply general tort law (TBK) principles, including: joint and several liability for co-tortfeasors (Articles 61–63 TBK); internal contribution rights; proportional liability based on fault. Thus, even without explicit PDPL provisions, joint controllership can be interpreted through general liability rules. However, this approach lacks the clarity and mandatory structure offered by the GDPR, creating uncertainty for compliance officers, lawyers, and institutions[109].

Joint Liability

Definition of Joint and Joint Liability

Joint liability arises when two or more persons are responsible for the same harmful act or for interconnected acts producing a common harm. Under Turkish law, the distinction between: joint liability arising from the same cause, and joint liability arising from different causes is relevant for determining contribution rights and internal apportionment[110].

In this respect, in personal data protection, these categories translate into: Same-cause liability: controllers jointly determine the purposes and means of the same processing[111]. Different-cause liability: controllers independently violate the law, and their separate violations collectively cause damage (e.g., inadequate security by one controller and unlawful transfer by another)[112].

The external and internal dimensions of joint liability differ[113].

External Relationship: Toward the Data Subject

In the external relationship, all controllers may be pursued for full compensation[114]. The data subject need not investigate internal responsibility allocation. Controllers may be held responsible regardless of their share in the processing operation. This is consistent with the GDPR and aligns with Turkish tort principles[115].

[109] Çetin, "Veri Sorumlusu…", p. 28

[110] Fikret EREN, *Borçlar Hukuku Genel Hükümler*, 28th ed., Yetkin Yayınları, Ankara, 2023, pp. 842–845 [in Turkish]..

[111] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 290.

[112] Kadem, "Ortak Veri Sorumlusu Kavramı…", pp. 1048–1050.

[113] Eren, *Borçlar Hukuku*, p. 848.

[114] Peter Blume, "Controller and processor: is there a risk of confusion?", (2013) 3(2) *International Data Privacy Law*, pp. 140–145.

[115] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 295.

Internal Relationship: Among Controllers

Internally, responsibility is divided based on: fault level, contribution to the harmful act, contractual arrangements, benefit derived from the processing[116]. For instance, a controller responsible for selecting an insecure IT infrastructure may bear greater internal responsibility. A controller that mishandles data subject requests may contribute to damage and thus owe compensation internally. These distinctions ensure fairness while maintaining robust protection for data subjects[117].

Joint Liability of Joint Data Controllers

Joint data controllers, by definition, influence essential aspects of processing. Therefore, their liability is inherently linked: If harm results from their joint decisions, liability is joint and several. If harm results from the stage of processing jointly controlled, each controller may be liable for that stage even if not responsible for subsequent independent processing by other parties. The Fashion ID case exemplifies this staged approach: The website operator was liable only for the collection and transmission phase. Facebook was responsible for subsequent autonomous processing[118]. In a similar interpretation applied in Turkey, if two controllers jointly collect personal data but one independently misuses it, the first controller may still be liable for the collection stage but not the subsequent misuse. However, because PDPL does not codify this structure, Turkish courts lack precise statutory guidance[119].

Joint Data Controllers' Compensation Obligations

Source of Compensation Obligations

Source of Joint Data Controllers' Compensation Obligations Compensation obligations arise from: unlawful processing, failure to ensure data security, failure to implement required technical/organizational measures, disclosure or transfer of data without a legal basis, failure to fulfill deletion/destruction obligations[120]. In this regard, under GDPR, the obligation to compensate is strict in nature: a controller is liable unless it proves that it is not in any way responsible for the event giving rise to damage. Under PDPL, liability is fault-based but

[116] Kadem, "Ortak Veri Sorumlusu Kavramı…", p. 1052.
[117] Çetin, "Veri Sorumlusu…", p. 31.
[118] Hayrunnisa Özzdemir, "Kişisel Verilerin Korunması Kanunu'nda Veri Sorumlusu ve Veri İşleyen Arasındaki İlişki ve Sorumluluk", (2020) 24(3) *AHBVÜHFD*, pp. 115–148 [in Turkish]; Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 385.
[119] Emel Badur – Nesibe Kurt Konca, "Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme", (2022) 13(2) *İnÜHFD*, p. 481 [in Turkish].
[120] Furkan Güven Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 2017, p. 199 [in Turkish].

interpreted broadly[121]. The existence of damage and a causal link is required; however, failure to fulfil explicit legal duties (e.g., security measures) may easily constitute negligence.

Damages Lawsuit

Damages Lawsuit Data subjects may seek: pecuniary damages (financial loss), and non-pecuniary damages (pain, distress, violation of personality rights).

Pecuniary Damage Claims

Pecuniary Damage Claims Pecuniary damages may include: financial losses from identity theft; economic losses caused by incorrect or outdated data; costs of remedying consequences of unlawful disclosure; expenses resulting from administrative or criminal consequences of inaccurate data[122]. Denial of credit due to inaccurate scoring information and employment loss due to wrongful data retention can be given as an example. Therefore, joint controllers may be jointly liable for these losses.

Non-Pecuniary Damages Claims

Non-pecuniary damages address: violation of privacy, reputational harm, emotional suffering[123]. In particular, Turkish law (TMK and TBK) provides broad protection for personal rights, enabling courts to award moral damages for violations arising from personal data misuse[124]. Importantly, moral damage claims are especially relevant in cases involving: sensitive data disclosure[125], unlawful profiling, reputational damage from search engine results, right to be forgotten violations[126]. Joint controllers may face significant moral damages awards, particularly where processing affects dignity, honour, or private life.

Conclusion

The increasing complexity of digital ecosystems has transformed the nature of personal data processing. Processing operations frequently involve multiple actors who jointly determine purposes and means, necessitating legal recognition

[121] Cem Süzek, "Veri Sorumlusunun Hukuki Sorumluluğu", (2019) *TBB Dergisi*; Arzu OĞUZ, "Hukuki Sorumluluk", (2017) *Banka ve Ticaret Hukuku Dergisi* [in Turkish].

[122] Eren, *Borçlar Hukuku*, p. 812; Uğur YİĞİT, *KVKK ve Uygulaması*, 2017, p. 210 [in Turkish].

[123] Tekin Memiş, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", (2017) *Beykent Üniversitesi Hukuk Fakültesi Dergisi*, p. 18 [in Turkish].

[124] Çiğdem KIRCA, "6098 sayılı Borçlar Kanunu ile Müteselsil Sorumluluk Konusunda Getirilen Yenilikler", in: *Yeni TBK Sempozyumu*, 2013, p. 24 [in Turkish].

[125] Ali Haydar Yağcioğlu, *Haksız Fiil Sebebiyle Aynı Zarardan Birden Fazla Kimsenin Müteselsil Sorumluluğu*, 2014, p. 38 [in Turkish].

[126] Serap Helvacı, *Kişilik Hakkı ve Korunması*, Legal Yayıncılık, İstanbul, 2021, p. 145 [in Turkish].; Ahmet KILIÇOĞLU, *Şahsiyet Hakkına Tecavüzden Doğan Sorumluluk*, Turhan Kitabevi, Ankara, 2020, p. 288 [in Turkish].

of joint data controllership. The GDPR explicitly codifies joint controllership, supported by extensive CJEU case law. Through cases such as Wirtschaftsakademie, Jehovah's Witnesses, and Fashion ID, the Court adopted a functional and expansive interpretation to ensure effective protection of individuals[127]. Turkish law, however, does not explicitly regulate joint controllership. Although PDPL's broad definition of "data controller" allows doctrinal recognition of joint controllership, the absence of explicit statutory provisions creates uncertainty regarding: allocation of obligations, disclosure duties, data subject rights handling, liability and contribution between controllers[128]. As a result, Turkish practice is inconsistent, and many organisations lack clarity regarding their obligations.[129]

This article demonstrates that Turkey should incorporate explicit rules on joint controllership—similar to GDPR Article 26—into the PDPL[130]. Such reform would enhance legal certainty, align Turkish law with international standards, and provide clearer guidance for data subjects, controllers, and courts. Joint data controllership enhances effective protection of personal data, but also imposes more extensive obligations and greater accountability on organisations. In an environment where digital services, state systems, and private infrastructures are increasingly interconnected, ignoring this reality undermines the coherence and effectiveness of personal data protection frameworks[131]. Since Turkish law primarily adopts fault-based liability for these cases, it will be necessary to establish fault on the part of joint data controllers for any damage caused. In conclusion, the concept of joint data controllers should be integrated into Turkish personal data protection law to meet current needs. However, its boundaries and scope must be applicable. In an era of increasing digitalization, personal data protection law should safeguard individuals' rights and freedoms without creating impractical responsibilities. When addressing this issue in personal data protection law, it is crucial to accurately identify joint data controllers, their

[127] Gernot Fritz – Nadia Paulus, "CJEU Rules on Joint Controllership: What Does This Mean for Companies?", Freshfields TQ Blog, 12 May 2024; Mesut Serdar Çekin, "Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Işığında Ortak Veri Sorumlusu Kavramı ve Hukuki Sonuçları", (2019) 35(2) *Batider*, p. 48 [in Turkish]; Court of Justice of the European Union (CJEU), Case C-210/16 (*Wirtschaftsakademie*), EU:C:2018:388; Case C-25/17 (*Jehovah's Witnesses*), EU:C:2018:551; Case C-40/17 (*Fashion ID*), EU:C:2019:629.

[128] Nilgün Başalp, "Kişisel Verilerin Korunması Hukukunda Veri Sorumlusu, Veri İşleyen ve Ortak Veri Sorumlusu", (2019) 1(1) *Kişisel Verileri Koruma Dergisi*, pp. 22–25 [in Turkish].

[129] Ömer Ekmekçi – Başak Baysal – İrem Yayvak Namlı, *Uygulamalı Tazminat Hukuku*, 2nd ed., Yetkin Yayınları, Ankara, 2022, p. 110 [in Turkish].

[130] Dülger, *Kişisel Verilerin Korunması Hukuku*, p. 370.

[131] Ayşe Selcen Atasoy, "6698 Sayılı Kişisel Verilerin Korunması Kanunu ve GDPR Kapsamında Veri Sorumlusu ve Veri İşleyen Kavramları", (2019) 77(2) *İstanbul Hukuk Mecmuası*, p. 755 [in Turkish].

relationships, and responsibilities, ensuring that these are applicable to each specific relationship[132].

Ethics

It is hereby declared that scientific and ethical principles were ashered to in the conduct and writing of this study, and that all sources used have been properly cited. The author did not use any generative AI tool for data analysis, coding, interpretation, or the generation of research findings. The author reviewed and approved all revisions and takes full responsibility for the manuscript's final content.

[132] Cem Süzek, "Kişisel Verilerin Korunması Kanunu Kapsamında Veri Sorumlusunun Hukuki Sorumluluğu", *TBB Dergisi*, S. 143, 2019, s. 330; Özdemir, Hayrunnisa, "Kişisel Verilerin Korunması Kanunu'nda Veri Sorumlusu ve Veri İşleyen Arasındaki İlişki ve Sorumluluk", *AHBVÜHFD*, C. 24, S. 3, 2020, s. 132.

References

Alsenoy, B. (2016). Liability under EU data protection law: From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and E-Commerce Law, 7*, 271–288.

Ardıç, Ş. (2018). Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 24*(2), 748–752.

Atasoy, A. S. (2019). 6698 sayılı Kişisel Verilerin Korunması Kanunu ve GDPR kapsamında veri sorumlusu ve veri işleyen kavramları. *İstanbul Hukuk Mecmuası, 77*(2), 755.

Ayözger, Ç. (2019). *Kişisel verilerin korunması hukuku: Elektronik haberleşme sektörüne ilişkin özel düzenlemeler dahil* (2nd ed.). Beta Basım Yayın.

Ayrancı, H., Çolak, A., & Özcan, O. (2022). *Kişisel Verilerin Korunması Kanunu şerhi*. Yetkin Yayınları.

Başalp, N. (2019). Kişisel verilerin korunması hukukunda veri sorumlusu, veri işleyen ve ortak veri sorumlusu. *Kişisel Verileri Koruma Dergisi, 1*(1), 22–25.

Blume, P. (2013). Controller and processor: Is there a risk of confusion? *International Data Privacy Law, 3*(2), 140–145.

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Colcelli, V. (2019). Joint controller agreement under GDPR. *EU and Comparative Law Issues and Challenges Series, 3*, 1030–1047.

Cordeiro, A. B. M. (2019). Civil liability for processing of personal data in the GDPR. *European Data Protection Law Review, 5*(4), 492–499.

Council of Europe. (1981). *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)*.

Council of Europe. (2018). *Convention 108+*.

Court of Justice of the European Union. (2018). *Case C-210/16, Wirtschaftsakademie, EU:C:2018:388*.

Court of Justice of the European Union. (2018). *Case C-25/17, Jehovah's Witnesses, EU:C:2018:551*.

Court of Justice of the European Union. (2019). *Case C-40/17, Fashion ID, EU:C:2019:629*.

Custers, B., & Gellert, R. (2012). Data protection as a fundamental right. *Computer Law & Security Review, 28*(3), 285–294.

Çekin, M. S. (2019). Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ışığında ortak veri sorumlusu kavramı ve hukuki sonuçları. *Batider, 35*(2), 48.

Çekin, M. S. (2022). *Kişisel verilerin korunması hukuku* (2nd ed.). On İki Levha Yayıncılık.

Çetin, S. (2020). Kişisel verilerin korunması hukukunda veri sorumlusu ve veri işleyen sıfatlarının belirlenmesi. *Bilişim Hukuku Dergisi, 2*(1), 15–31.

Data Protection Board. (n.d.). *Data Protection Board decisions*.

Dülger, M. V. (2016). Unutulma hakkı: Dijital hafızadan silinmeyi istemek. *Terazi Hukuk Dergisi*, 120.

Dülger, M. V. (2020). *Kişisel verilerin korunması hukuku* (3rd ed.). Hukuk Akademisi.

Eren, F. (2023). *Borçlar hukuku genel hükümler* (28th ed.). Yetkin Yayınları.

European Data Protection Board. (2021). *Guidelines 07/2020*.

European Parliament and Council. (1995). *Directive 95/46/EC*.

European Parliament and Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*.

Evre, Ö. (2021). Veri taşınabilirliği hakkı ve Türk hukuku bakımından değerlendirilmesi. *İstanbul Hukuk Mecmuası, 79*(1), 140.

Finck, M. (2021). Cobwebs of control: The two imaginations of the data controller in EU law. *International Data Privacy Law, 11*(4), 333–347.

Fritz, G., & Paulus, N. (n.d.). CJEU rules on joint controllership: What does this mean for companies? *Freshfields TQ Blog*. Retrieved May 12, 2024.

Helvacı, S. (2021). *Kişilik hakkı ve korunması*. Legal Yayıncılık.

Hess, B. (n.d.). *The unclaimed territory of the GDPR: Joint controllership and liability*.

Ivanova, Y. (2020). Data controller, processor or a joint controller. In M. Tzanou (Ed.), *Personal data protection and legal developments in the European Union*.

Kadem, M. B. (2020). 6698 sayılı Kanun kapsamında ortak veri sorumlusu kavramı ve hukuki sorumluluk. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 26*(2), 1012–1052.

Kaya, İ. (2023). *Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) kapsamında ortak veri sorumluluğu* [Master's thesis, Hacettepe University].

Kılıç, A. G. (2020). Avrupa Birliği Adalet Divanı kararları ışığında ortak veri sorumluluğu. *Hukuk Köprüsü*, 18, 42–58.

Kılıçoğlu, A. (2020). *Şahsiyet hakkına tecavüzden doğan sorumluluk*. Turhan Kitabevi.

Knetsch, J. (2022). The compensation of non-pecuniary loss in GDPR infringement cases. *Journal of European Tort Law, 13*(2).

Kuner, C. (2007). *European data protection law: Corporate compliance and regulation* (2nd ed.). Oxford University Press.

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Küzeci, E. (2020). *Kişisel verilerin korunması* (5th ed.). On İki Levha Yayınları.

Law No. 6698 on the Protection of Personal Data. (2016).

Lynskey, O. (2014). Deconstructing data protection. *International and Comparative Law Quarterly, 63*, 569.

Personal Data Protection Board. (2020). *Decision No. 2020/481*.

Room, S. (2007). *Data protection & compliance in context*. The British Computer Society.

Tran, D., & Adde, L. (2019). Joint controller relationships: More prevalent than previously thought? *Privacy & Data Protection*, *19*(8), 6–8.

Turkish Civil Code. (n.d.).

Turkish Penal Code, arts. 135–138. (n.d.).

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.