Joint Controllership Under the GDPR - Concept, Responsibilities, and Liability

Assistant professor **Ayça ZORLUOĞLU YILMAZ**[1]

Abstract

This article explores the concept of joint controllership and the liability regime of joint controllers. In the current era, the importance of personal data is increasing and these personal data are processed and determined by more and more people with common purposes and means. This situation also gives rise to the concept of joint controllership. When personal data is processed, the issue of who will be liable for which damage and to what extent in the event of damage to the data subject has gained importance. For this reason, the issue of liability of joint controllers should be emphasized. This article thus consists of four main sections. The first section presents the historical background of the concept of joint controllership. The second section comprehensively outlines the definition of joint controllership by considering the relevant CJEU decisions on the subject. The third section explores the responsibilities of joint controllers. The fourth section sketches and discusses the liability of joint controllers. The liability of the joint controller, which has minimal fault in the occurrence of the damage and occupies a very small place in the balance of power compared to the other joint controllers, has also been evaluated.

Keywords: *joint controllership, GDPR, CJEU, responsibility, joint and several liability, controller.*

JEL Classification: *K13, K15, K33*

DOI: 10.62768/TBJ/2025/15/1/06

Please cite this article as:	**Article History**
Zorluoğlu Yılmaz, Ayça, 'Joint Controllership Under the GDPR - Concept, Responsibilities, and Liability', *Juridical Tribune – Review of Comparative and International Law* 15, no. 1 (March 2025): 93-107.	Received: 25 September 2024 Revised: 15 November 2024 Accepted: 10 January 2025

1. Introduction and historical background of joint controllership

The value of personal data is increasing day by day. In the digital age we are in, processing personal data has become inevitable. However, it is of great importance not to violate personal rights while processing personal data. As the processing of personal data becomes widespread, the actors and activities in this area are also expanding. The Regulation (EU) 2016/679 (General Data Protection Regulation-GDPR), which entered into force in 2018 for uniformity in the processing of personal data, is of great importance. Joint controllership has been legally regulated with the

[1] Ayça Zorluoğlu Yılmaz - Faculty of Law, Hacettepe University, Ankara, Turkey, ORCID No.: 0000-0001-7250-4097, azorluoglu@hacettepe.edu.tr.

GDPR. GDPR sheds light on the legal systems of many countries, whether they are members of the Union or not, regarding the protection of personal data. For example, Turkish law, which is not a member of the EU but takes GDPR as its basis for regulations on the protection of personal data, although the concept of joint controllership has not been accepted in the Law on the Protection of Personal Data No. 6698, joint controllership has been accepted with the decisions made by the Personal Data Protection Board, which is the regulatory institution for the protection of personal data, as a result of the development of technology[2]. This situation also shows that joint controllership may become even more important with a possible change in the law in the future. For this reason, what joint controllership is, in what cases it arises and the nature of this concept should be investigated.

The concept of personal data was first accepted in 1981 with Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[3]. This Convention obliges member countries to make legal arrangements regarding the automatic processing of personal data belonging to real persons[4]. In 2018, in order to bring this Convention into line with current developments, Convention 108 + Convention for The Protection of Individuals with Regard to the Processing of Personal Data was adopted[5].

In the European Union law, the protection of personal data of individuals is accepted as a fundamental human right and the free movement of data within the member states is made possible by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the

[2] Personal Data Protection Board's Principle Decision dated 23/12/2021 and numbered 2021/1304 on "Creation of a blacklist program that enables the processing of data of the relevant persons by the software developers and sellers of car rental programs and the sharing of this data between car rental companies", https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf. According to the relevant decision, the Personal Data Protection Board has received reports of blacklisting practices in the car rental sector. Accordingly, car rental companies compile the personal data of their car rental customers as a list of the negative situations that occur during the use of the vehicles and share them with other car rental companies using the same software. Car rental companies cannot intervene in the software of the database in question, but they transfer data to this database. This data can also be accessed by other car rental companies using the same software. The Board has accepted car rental companies as data controllers. The novelty aspect of the decision is that it has accepted car rental companies that can use the blacklist record in the software, which is considered personal data, for their own benefit and software companies as joint controllers. The Board has used certain criteria when determining joint controllers: a) who is the first and last user of the data, b) who enters the data, c) for what purpose the data entry is made, d) who is authorized to change, delete and transfer the data, e) what activities the data controllers carry out with the processed data. The criteria for determining joint controllership in the decision are not limited but are given as examples. The decision is important in that it is the first time that joint controllership has been accepted in Turkish law.

[3] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", European Treaty Series - No. 108, January 28, 1981, https://rm.coe.int/1680078b37.

[4] Dülger, Murat Volkan. *Kişisel Verilerin Korunması Hukuku [Personal Data Protection Law]* (Hukuk Akademisi Yayınları, 2019), 55.

[5] "Convention 108 + Convention for the protection of individuals with regard to the processing of personal data", June 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

Processing of Personal Data and on the Free Movement of Such Data[6]. Although this Directive is important in terms of establishing a general understanding of data protection within the European Union, due to the differences that occurred during the adoption into the domestic laws of the member states, uniformity in the protection of personal data within the Union could not be achieved[7]. Thereupon, a need for a new regulation arose and the much more comprehensive GDPR came into force in 2018. Thus, Directive 95/46/EC was repealed. The aim of the GDPR is to ensure uniformity with Regulation regarding the protection of personal data[8].

The definition of personal data is regulated in GDPR Art. 4(1). Accordingly, personal data is defined as all information belonging to an identified or identifiable natural person. GDPR Art. 4(1) lists the cases used to determine personal data as examples. Accordingly, any information belonging to a natural person can be personal data, and it is not even necessary for this data to be true or accurate[9]. Processing of personal data is defined under Art. 4(2) of GDPR. Under GDPR Art. 4(1), "data subject" refers to an identified or identifiable natural person whose data is processed.

Under GDPR Art. 4 (7), the controller is defined as a natural or legal person, a public institution, or other organization that determines the purpose and meaning of the processing of personal data, either alone or together with others. The scope of the legal person controller may include the State, public institutions, schools, local authorities, fire departments, police forces, associations, foundations, companies, banks, insurance companies, law firms, supermarkets, opticians, pharmaceutical companies, telecommunications companies including internet service providers, internet search engines, hospitals, biobanks, etc.[10]. If the controller is a natural person, an important

---

[6] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", 24 October 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[7] Dülger, Personal Data, 59, 65; Küzeci, Elif. Kişisel Verilerin Korunması [Protection of Personal Data] (On İki Levha Yayıncılık, 2020), 186, 221; Nilgün Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri [Key Innovations of the European Union General Data Protection Regulation]" " *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 21, no.1 (2015): 77-106, 81, 82, https://dergipark.org.tr/tr/download/article-file/271091.

[8] Sophie Stalla-Bourdillon/ Henry Pearce and Niko Tsakalakis, "The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify", *Computer Law & Security Review* 34, no.4 (2018): 785, https://doi.org/10.1016/j.clsr.2018.05.012; Başalp, "General Data Protection", 85; Ayşe Nur Akıncı, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi [The Innovations Introduced by the European Union General Data Protection Regulation and its Evaluation in Terms of Turkish Law]", *T.C. Kalkınma Bakanlığı Çalışma Raporu-6*, June 2017, 14, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf.

[9] Mac Macmillan, "Data Protection Concepts", in *European Data Protection Law and Practice,* ed. Eduardo Ustaran. (Iapp Publication, 2018), 82.

[10] Damien Welfare and Peter Carey, "Territorial Scope and Terminology" in *Data Protection A Practical Guide to UK and EU Law*, ed. Peter Carey (Oxford University Press, 2018), 18; Valentina Colcelli, "Joint Controller Agreement Under GDPR", *EU and Comparatıve Law Issues and Challenges Series,* no.3 (2019): 1030, https://hrcak.srce.hr/ojs/index.php/eclic/article/view/9043/5125; Jenna Mäkinen, "Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things", I*nformation & Communications Technology Law* 24, no.3 (2015): 272, http://dx.doi.org/10.1080/13600834.2015.1091128.

exceptional provision is regulated in the processing of personal data. According to GDPR Art. 2(2) and Recital 18; it has been accepted that if personal data is processed by a natural person solely within the scope of activities related to him/herself or his/her household, without being connected to a professional or commercial activity, the provisions of the GDPR will not be applied. However, persons such as social media platforms and search engines[11] that provide tools for the processing of such personal and household data are still considered as controllers and the provisions of the Regulation continue to apply to them.

The concept of joint controller is regulated in GDPR Art. 26. Joint controllership is a type of data responsibility in which two or more data controllers jointly determine the purposes and means of processing personal data. At this point, in order to more clearly reveal the concept of joint controllership, it is necessary to look at its definition and historical background.

2. The definition of joint controllership and the relevant CJEU decisions

2.1. The definition of joint controllership

There was no concept of joint controllership in Convention No. 108. In the Convention No. 108 + Art. 2, which is the updated version of this Convention, it is stated with the expression co-controller that there may be more than one controller who can participate in different stages of data processing[12]. The concept of joint controllership is included in 95/46/EC. However, due to the non-compulsory nature of the Directive for member states, joint controllership has not been properly reflected in the domestic laws of all member states[13]. The concept of joint controller is defined in detail in GDPR Art. 26, and its procedures and principles are regulated. According to GDPR, a system has been adopted in which the controller is primarily responsible for data protection activities[14]. While it is easier to determine the responsible person when there is a single controller, it becomes more difficult to determine the responsible person when the number of people involved in the data processing activity increases. For this reason, the provisions regulated under GDPR Art. 26 are important for determining liability. According to GDPR Art. 26, it is regulated that joint controllership will arise when two or more controllers act together in determining the purposes and means of

[11] İrem Kaya, *KVKK ve GDPR Kapsamında Ortak Veri Sorumluluğu [Joint Data Controllership under KVKK and GDPR]* (On İki Levha Yayıncılık, 2023), 24.

[12] "Convention 108 + Convention for the protection of individuals with regard to the processing of personal data", June 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1, 17.

[13] Christopher Kuner, *European Data Protection Law: Corporate Regulation and Compliance* (Oxford University Press, 2007), 70.

[14] Veronique Cimina, "The data protection concepts of 'controller', 'processor' and 'joint controllership' under Regulation (EU) 2018/1725", *ERA Forum* 21, (2021):639–654, https://link.springer.com/article/10.1007/s12027-020-00632-8, 645; Benjamin Wong, "Problems With Controller-Based Responsibility in EU Data Protection Law", *International Data Privacy Law*, Volume 11, Issue 4, (2021): 375–387, https://doi.org/10.1093/idpl/ipab014, 375, 376.

data processing. The act of jointly determining the purposes and means of processing data does not have to occur at the same or a single point in time, and it is not required for the parties to contribute equally. The existence of joint controllership should be determined by considering the characteristics of the underlying factual circumstances[15].

The GDPR system imposes certain duties and obligations on data controllers, and controllers must ensure that these obligations are not violated. As a rule, each controller is responsible for its actions, but one of the most fundamental exceptions to this rule is joint controllership. In joint controllership, a data controller might also be held accountable for the actions and operations of other data controllers involved[16].

Every data processing activity involving multiple actors does not lead to joint controllership. In joint controllership, it is essential that multiple data controllers jointly determine the purposes and means of one or more processing activities, in other words, the decision-making process. In some cases, especially in practice, it may be difficult to distinguish between "joint" and "separate" control. The decisive factor is whether the different parties jointly determine the purposes and means of the processing activity in question. If the parties do not pursue the same purposes or do not use the same means to achieve them, the relationship between them is probably one of "separate controllers" rather than "joint controllers". However, if the data controllers jointly determine the purposes and means of the data processing activity, then joint controllership is the case[17]. This can be in the form of a common decision by two or more data controllers, or it can be in the form of a converging decision where these actors complement each other through purposes and means[18]. In joint controllership that occurs in the form of converging decisions, actors are considered joint controllers not for the entire data processing activity, but only for the parts where they jointly determine the purpose and means. If one of the actors makes decisions about a stage of the data processing activity alone, they are solely liable for that part[19].

---

[15] Macmillan, Data Protection, 76.; Colcelli, "Joint Controller Agreement Under GDPR", 1033; Mäkinen, "Data quality", 272; European Data Protection Board. "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", European Data Protection Board, adopted on 07 July 2021, accessed September 5, 2024, https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_ 202007_controllerprocessor_final_en.pdf, para.51, 52.

[16] Stephan Hess, "The GDPR: Joint Controllership and Independent Controllership Should the SWIFT criteria determine the difference?" (Thesis, Tilburg University, 2019), 13; Brendan Van Alsenoy, "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation" *JIPITEC* 7, no. 3 (2016): 271- 288, https://www.jipitec.eu/archive/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf, 281.

[17] Van Alsenoy, "Liability", 280; "EDPB Guidelines", para. 51, 53; Stalla-Bourdillon Pearce and Tsakalakis, "The GDPR: A game changer", 800.

[18] Cimina, "The data protection concepts of 'controller', 'processor' and 'joint controllership' under Regulation (EU) 2018/1725", 645; Kaya, *Joint Data*, 46, 47; Cyril Fischer, "Re-thinking the allocation of roles under the GDPR in the context of cloud computing", *International Data Privacy Law* 14, no.4 (2024): 55, 56, 63, https://doi.org/10.1093/idpl/ipad023; Jennifer Cobbe and Jatinder Singh, "Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges", *Computer Law & Security Review*, no. 42 (2021):12, https://doi.org/10.1016/j.clsr.2021.105573; "EDPB Guidelines", para. 54.

[19] "EDPB Guidelines", para. 57.

2.2. The relevant CJEU decisions

While joint controllership is regulated in the GDPR, its scope is being determined by the decisions of the Court of Justice of the European Union (CJEU). In particular, three decisions known as *Wirtschaftsakademie Schleswig-Holstein*, *Jehovan todistajat*, and *Fashion ID* are cornerstones in this regard.

2.2.1. Court of Justice of the European Union Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie SchleswigHolstein GmbH, Facebook Ireland Limited*

Wirtschaftsakademie is an organization that provides educational services through its fan page on Facebook. Fan pages are pages on Facebook that can be used and interacted with by real and legal persons. The administrators of these fan pages can obtain anonymous statistical data about the people who visit their pages with the Facebook Insights extension provided by Facebook under non-negotiable conditions. This data is collected through cookies and stored for two years.

The data protection authority of the German Land of Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*) has ruled that Wirtschaftsakademie and Facebook Ireland are joint controllers and have failed to comply with their obligation to inform about the personal data they collect through cookies. Wirtschaftsakademie appealed the decision and claimed that the data had been collected by Facebook. The competent authority, which assessed the appeal, ruled that Wirtschaftsakademie is a joint controller because the data was collected through a service that Facebook only offers to fan page administrators. Moreover, it uses the same data processing tools for the same purpose, and it actively and knowingly contributes to the collection of data. The CJEU has also ruled that Wirtschaftsakademie is a joint controller with Facebook because it accepts the services offered by Facebook in order to reach its target audience and contributes to the collection of personal data belonging to users. Because the Wirtschaftsakademie obtained the personal data of users for the same purposes, using the same parameters and tools as Facebook, and ruled that it is not necessary for all joint controllers to have access to all personal data in order for joint controllership to exist[20].

This decision is important because the CJEU ruled that for joint controllership, joint controllers do not need to share responsibility equally. In addition, this decision aims to increase the protection of personal data on social media platforms[21].

[20] Court of Justice of the European Union Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie SchleswigHolstein GmbH, Facebook Ireland Limited, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62016CJ0210, para. 14-17, 38, 39, 40.
[21] Court of Justice of the European Union Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie SchleswigHolstein GmbH, Facebook Ireland Limited, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62016CJ0210, para. 42, 43.

2.2.2. Court of Justice of the European Union Case C-25/17 *Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta*

Members of Jehovah's Witnesses Community, a religious community, met people face to face in Finland and recorded personal data such as addresses, family members, and religious views for later use[22]. Through these notes, maps of the areas where information was collected were made, as well as lists of people who refused to join the community[23].

The Finnish Data Protection Board prohibited the Community from doing this. Following an appeal against the decision, the Finnish Administrative Court ruled that Johovah's Witnesses Community was not a data controller[24]. The Finnish Supreme Administrative Court then brought the matter before the CJEU. The CJEU ruled that the Community and its members decide how personal data will be collected and processed, and therefore they should be considered joint controllers[25]. In this decision, the CJEU reiterated its view that for joint controllership to exist, it is not necessary for all data controllers to have access to all data and that the responsibilities of joint controllers do not need to be equal[26].

2.2.3. Court of Justice of the European Union Case C-40/17 *Fashion ID GmbH & Co. KG, Facebook Ireland Limited v. Verbraucherzentrale NRW e.V., Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*

Fashion ID, an online clothing company, has added Facebook's Like button to its website. This way, IP addresses and user information belonging to people visiting the site are transferred to Facebook, regardless of whether they are Facebook members or whether they click on the Like button[27]. The owner of the clothing company's website

[22] Court of Justice of the European Union Case C-25/17 Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0025, para.15.

[23] Court of Justice of the European Union Case C-25/17 Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0025, para.16.

[24] Court of Justice of the European Union Case C-25/17 Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0025, para.11-13.

[25] Court of Justice of the European Union Case C-25/17 Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0025, para.75.

[26] Court of Justice of the European Union Case C-25/17 Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0025, para.66.

[27] Court of Justice of the European Union Case C-40/17 Fashion ID GmbH & Co. KG, Facebook Ireland Limited v. Verbraucherzentrale NRW e.V., Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0040, para. 27.

does not control what data is collected by this plugin or what Facebook does with this data[28].

In its decision on the subject, the CJEU ruled that Fashion ID and Facebook were joint controllers on the grounds that although the Fashion ID site had no influence on the collection of personal data by Facebook, it contributed to the collection of personal data by adding the plugin that enables the collection of this data. Because Fashion ID added the Like button to its site due to its economic interests and was aware that the data was being transmitted to Facebook, it was accepted as a joint controller[29]. At this point, Fashion ID should inform its users about the data collected and obtain their consent[30].

3. The responsibilities of joint controllers

According to GDPR Art. 26, joint controllers must determine their responsibilities within the scope of this activity in some sort of arrangement, i.e. an agreement. In this context, joint controllers must transparently, and understandably set out their roles at different stages of data processing and their responsibilities related to them. In this way, the rights of data subjects are tried to be protected[31]. The data subject must be informed about the essence of this arrangement[32]. According to Article 26 of GDPR, it must be clearly stated which joint controller has the obligation to provide information on the data subject's rights and, in particular, the rights regulated in Articles 13 and 14. Under the arrangement, joint controllers may appoint a point of contact that data subjects can reach in case of need.[33].

All joint controllers are obliged to ensure that all activities carried out comply with the GDPR rules. Accordingly, all joint controllers are responsible for ensuring that other data controllers comply with all their general obligations under the GDPR. According to the non-exhaustive list provided by the EDPB, joint controllers are

[28] Court of Justice of the European Union Case C-40/17 Fashion ID GmbH & Co. KG, Facebook Ireland Limited v. Verbraucherzentrale NRW e.V., Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0040, para. 26.

[29] Court of Justice of the European Union Case C-40/17 Fashion ID GmbH & Co. KG, Facebook Ireland Limited v. Verbraucherzentrale NRW e.V., Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0040, para. 76-81.

[30] Court of Justice of the European Union Case C-40/17 Fashion ID GmbH & Co. KG, Facebook Ireland Limited v. Verbraucherzentrale NRW e.V., Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0040, para. 106.

[31] "EDPB Guidelines", para. 161, 162, 177; Colcelli, "Joint Controller Agreement Under GDPR", 1030, 1038; Jiahong Chen/ Lilian Edwards/ Lachlan Urquhart and Derek McAuley, "Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption", *International Data Privacy Law* 10, no.4 (2020):282, 291, https://doi.org/10.1093/idpl/ipaa011; Cobbe and Singh, "Artificial intelligence as a service", 13; Cimina, "The data protection concepts of 'controller', 'processor' and 'joint controllership' under Regulation (EU) 2018/1725", 646, 647.

[32] "EDPB Guidelines", para. 179- 181.

[33] "EDPB Guidelines", para.182- 185.

obliged to take the necessary measures in addition to the obligations set out in GDPR Art 26, *"implementation of general data protection principles, legal basis of the processing, security measures, notification of a personal data breach to the supervisory authority and to the data subject, data protection impact assessments, use of a processor, transfers of data to third countries, organization of contact with data subjects and supervisory authorities"*[34]. For this reason, responsibilities and their distribution should be evaluated on a case-by-case basis[35].

Joint controllers are obligated, within the scope of processing activities covered by this responsibility, to act in accordance with the principle of purpose limitation and to ensure that appropriate measures are taken to secure the personal data processed within the framework of shared tools. Each joint controller must keep a record of processing activities or appoint a Data Protection Officer. Joint controllers are also obliged to implement appropriate technical and organizational measures to ensure that processing activities meet the requirements of the GDPR. To this end, data controllers must use processors that provide sufficient safeguards. Factors to be taken into account when determining the appropriate processor include; the processor's security measures and technical expertise in data breaches, the processor's reliability and resources, and the processor being subject to an approved certification mechanism[36].

4. Liability of joint controllers

Liability is the responsibility of one or more persons for the damage caused to another. Although the concept of joint controllership is defined in GDPR Art. 26, the CJEU has not made a clear case law in its decisions on what the responsibilities of joint controllers that lead to liability are. For this reason, it is not clear exactly what the responsibilities of joint controllers are from the CJEU's perspective[37]. Under GDPR Art. 82 it is regulated that in case of joint controllership, if the persons concerned are harmed by this processing activity, each of the joint controllers will be jointly liable for the entirety of this damage. In this way, if more than one person is liable for the same damage for the same or several reasons, it is a case of joint and several liability[38].

---

[34] "EDPB Guidelines", para. 166.

[35] Fischer, "Re-thinking the allocation of roles", 64.

[36] "EDPB Guidelines", para. 167, 168, 170.

[37] Monika Zalnieriute and Genna Churches, "When a 'Like' Is Not a 'Like': A New FragmentedApproach to Data Controllership", *The Modern Law Review* 84, no.4 (2020): 869, 870, doi: 10.1111/1468-2230.12537; Jure Globocnik, "On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID Directive 95/46/EC, Arts. 2(d) and (h), 7(a) and (f), 10", *International Review of Intellectual Property and Competition Law*, no.50 (2019): 1038, https://doi.org/10.1007/s40319-019-00871-4.

[38] Karl Oftinger and Emil W. Stark, *Schweizerisches Haftpflichtrecht [Swiss liability law], Erster Band: Allgemeiner Teil* (Schulthess Polygraphischer Verlag), 1995, 488, 489; Heinz Rey, *Ausservertragliches Haftpflichtrecht* Haftpflichtrecht *[Non-contractual liability law]*, (Schulthess, 2008), 323, 329, 330; Claire Huguenin, *Obligationenrecht [Law of obligations], Allgemeiner Teil* (Schulthess, 2006), 224, 225; Peter Gauch/ Walter R. Schluep/ Jörg Schmid /Heinz Rey and Susan Emmenegger, *Schweizerisches Obligationenrecht [Swiss law of obligations], Allgemeiner Teil,* (Schulthess, 2008), 297, 298; Fikret Eren, *Borçlar Hukuku Genel Hükümler [General Provisions of Law of Obligations]* (Yetkin Yayınları, 2018),

The purpose of joint and several liability is to provide special protection for the victim who has suffered harm caused by more than one person. In this way, by ensuring that there are multiple liable parties in front of the victim, it aims to strengthen the position of the injured party. This is because the association among joint controllers who carry out the data processing activity that causes the harm carries a greater potential risk compared to the behaviors of a single person[39]. Moreover, this purpose is clearly stated in GDPR Art 82. According to GDPR Art 82/4, each of the joint controllers is held liable for the entirety of any damage arising from the processing activity.

The difference between joint controllership and data controllership is that the rules regarding the protection of personal data and the obligations related to them must be shared among the joint controllers[40].

In joint and several liability, as more than one person jointly causes the same harm, the relationship between the injurers and the injured parties is called the external relationship, while the relationship among the injurers themselves is referred to as the internal relationship. In joint and several liability, the position of the injurers who jointly caused the harm is equal in relation to the injured party. The injured party may pursue any of the jointly and severally liable parties for compensation. The liability of the injurers continues until the entire harm is compensated. Even if jointly and severally liable parties have reached an agreement regarding the division of liability, this does not affect the injured party in the external relationship. The injured party may claim compensation for their damage from all liable parties or any of them. Joint and several liability protects the injured party by allowing them to claim their entire compensation from any jointly and severally liable parties.

Similarly, the possibility of filing a claim against only one jointly and severally liable party also ensures procedural economy for the injured party, as they can recover the entire compensation in a single lawsuit, which facilitates the burden of proof. In other words, this has a protective effect on the injured party in terms of procedural efficiency. The jointly and severally liable party who has been pursued for compensation cannot demand that the damage be claimed or compensated from the other liable parties instead[41]. To the extent that each of the joint controllers that caused the damage terminates its compensation obligation through performance or exchange,

834; Colcelli, "Joint Controller Agreement Under GDPR", 1039, 1040; Stalla-Bourdillon Pearce and Tsakalakis, "The GDPR: A game changer", 800; Klaus Wiedemann, "Profiling and (automated) decision-making under the GDPR: A two-step approach", *Computer Law & Security Review*, no.45 (2022): 11, https://doi.org/10.1016/j.clsr.2022.105662.

[39] Oftinger and Stark, *Schweizerisches Haftpflichtrecht,* 491, 492; Huguenin, *Obligationenrecht,* 226; Rey, *Ausservertragliches Haftpflichtrecht*, 324; Eren, *Law of Obligations*, 843; Kaya, *Joint Data*,94, 95; Stalla-Bourdillon Pearce and Tsakalakis, "The GDPR: A game changer", 805; Globocnik, "On Joint Controllership", 1038.

[40] "EDPB Guidelines", para 48; Colcelli, "Joint Controller Agreement Under GDPR", 1040, 1041.

[41] Gauch/Schluep/Schmid/Rey and Emmenegger, *Schweizerisches Obligationenrecht,* 299- 302; Huguenin, *Obligationenrecht,* 226, 227; Rey, *Ausservertragliches Haftpflichtrecht,* 343- 348; Eren, *Law of Obligations*, 843.

the other joint controllers will also benefit from this and will be relieved of the debt to this extent[42].

The allocation of liability among joint controllers pertains to the internal relationship between them. A joint controller who compensates the injured party can seek recourse from the other joint controllers for any amount paid exceeding their share of liability and can succeed to the rights of the injured party in this regard. In other words, each joint controller, as a jointly liable party, may request the excess payment from the other joint controllers. In determining the shares of liability among the jointly liable parties, factors such as each party's fault and the degree of risk created by this fault are considered based on the specifics of the case. The severity of the fault may range from slight negligence to intent. Therefore, the party that has intentionally caused the damage will bear a heavier share of liability in the internal relationship. Additionally, the intensity of the danger created by those who caused the damage together should also be taken into account. If one party's actions, activities, or operations have significantly increased the likelihood and severity of the harmful outcome, their liability should be assessed more heavily[43]. In other words, if the processing behavior of one of the joint controllers has been more influential in causing the harmful outcome compared to the behavior of the other joint controller, then the liability for compensation in the internal relationship should be assigned more heavily to the more impactful party. This allocation of liability within the internal relationship should be evaluated by considering each case and its unique circumstances among the joint controllers.

The European Data Protection Board has accepted that joint liability continues even when one of the parties to joint control is a large service provider and the other is a much smaller data controller. According to the EDPB's perspective, a small data controller must still assess the conditions in any case, and, since it freely accepts these conditions and benefits from the service, it must comply with the GDPR's data protection requirements. This implies that all joint controllers are assumed to accept full liability. According to the Court of Justice of the European Union (CJEU), if a data controller is aware of data processing activities and fully understands the situation, this awareness is sufficient for the liability to arise. Similarly, in the Fashion ID case, the CJEU determined that consenting to benefit from a commercial advantage is sufficient to establish liability[44]. Although the consent given by the data controller is seen as a sufficient criterion for the emergence of liability, it should also be considered how this consent is given. For example, it should be evaluated whether the consent given by a very small and weak data controller is free and informed in the face of a very powerful data controller. Because there is a power asymmetry[45] between these parties and the

---

[42] Eren, *Law of Obligations*, 843.

[43] Oftinger and Stark, *Schweizerisches Haftpflichtrecht,* 492, 493, 503; Gauch/Schluep/Schmid/Rey and Emmenegger, *Schweizerisches Obligationenrecht*, 302, 303, 304; Huguenin, *Obligationenrecht,* 227; Eren, *Law of Obligations,* 847, 848; Kaya, *Joint Data*, 102; Wiedemann, "Profiling and (automated) decision-making under the GDPR", 11.

[44] "EDPB Guidelines", para. 110; Fischer, "Re-thinking the allocation of roles", 57.

[45] Fischer, "Re-thinking the allocation of roles", 59, 60.

agreement regarding the allocation of liability may have been imposed by the powerful party on the other without proper negotiation. In such cases, there is often a "take it or leave it" situation. Although the CJEU aims to protect the injured parties in all circumstances by holding all joint controllers jointly liable to third parties, it should not be overlooked that this approach could lead to results that may be unfair in specific cases. The GDPR holds joint controllers accountable for each other's activities. But when one party is a very large and powerful data controller, it becomes nearly impossible for the smaller controller to monitor or influence the larger one. Consequently, the smaller joint controller may also be unable to fulfill the obligations envisioned by the GDPR[46].

5. Conclusion

In the CJEU decisions, the concept of joint controller is interpreted particularly broadly in order to protect the data subjects whose data are processed more effectively. Joint controllership should be determined according to the parties' actual control over the purposes and means of data processing. This approach is also in line with GDPR Art 28, which provides that the data processor shall be deemed to be the data controller in cases where the processor is in a position to determine the purposes and means of data processing activities beyond the instructions of the controller. In such a case, the data processor and controller may even become joint controllers.

According to the case law established by the CJEU rulings, the fact that each joint controller does not have access to the processed personal data does not prevent the formation of joint controllership. But it may affect the extent of each party's liability. For joint controllership to be present, it is not necessary for the joint controllers to bear equal responsibility. Since the parties to joint controllership may participate in different stages or at different levels of the data processing activity, their levels of responsibility should be determined based on the specifics of each case. Additionally, for joint controllership to exist, all data controllers must jointly decide on the purposes and means of processing. At this point, it is important to consider whether all controllers have determined the essential means of data processing. Essential data processing means are elements closely related to the purpose and scope of data processing, such as which personal data will be processed, how long they will be stored, and which data will be transferred.

The GDPR stipulates that joint controllers are considered jointly and severally liable for the data processing activities they undertake together. Thus, data subjects whose rights have been infringed can pursue any of the joint controllers in the external relationship and seek compensation for damages. This approach aims to provide the broadest possible protection for data subjects. In the internal relationship, however, a joint controller who pays more than their share due to the fault of another can seek recourse from the others for the excess amount paid. This concept aligns with the principle of joint and several liability recognized in general legal systems.

[46] Fischer, "Re-thinking the allocation of roles", 60.

If a data controller is aware of data processing activities and fully understands the situation, this awareness is enough for the liability to arise. Although the consent given by the data controller is seen as a sufficient criterion for the emergence of liability, it should also be considered how this consent is given. It should be evaluated whether the consent given by a very small and weak data controller is free and informed in the face of a very powerful data controller. Because an agreement on the allocation of responsibility between parties with a power asymmetry may have been imposed by the more powerful party on the other without proper negotiation. Even the GDPR holds joint controllers accountable for each other's activities, when one party is a very large and powerful data controller, it becomes nearly impossible for the smaller controller to impact the larger one.

The EU regulators should pay greater attention to this issue under the current situation. Therefore, a smaller and weaker data controller must carefully review what they are consenting to and ensure that the liability-sharing aligns with their interests.

Bibliography

1. Akıncı, Ayşe Nur. "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi [The Innovations Introduced by the European Union General Data Protection Regulation and its Evaluation in Terms of Turkish Law]", *T.C. Kalkınma Bakanlığı Çalışma Raporu-6*, June 2017, 14, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf.
2. Başalp, Nilgün. "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri [Key Innovations of the European Union General Data Protection Regulation]" *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 21, no.1 (2015): 77-106, https://dergipark.org.tr/tr/download/article-file/271091.
3. Chen, Jiahong, Lilian Edwards, Lachlan Urquhart and Derek McAuley. "Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption", *International Data Privacy Law* 10, no.4 (2020):279- 293, https://doi.org/10.1093/idpl/ipaa011.
4. Cimina, Veronique. "The data protection concepts of 'controller', 'processor' and 'joint controllership' under Regulation (EU) 2018/1725", *ERA Forum* 21, (2021):639–654, https://link.springer.com/article/10.1007/s12027-020-00632-8.
5. Cobbe, Jennifer and Jatinder Singh. "Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges", *Computer Law & Security Review*, no. 42 (2021):1- 25, https://doi.org/10.1016/j.clsr.2021.105573.
6. Colcelli, Valentina. "Joint Controller Agreement Under GDPR", *EU and Comparatıve Law Issues and Challenges Series*, no. 3 (2019): 1030-47, https://hrcak.srce.hr/ojs/index.php/eclic/article/view/9043/5125.
7. Convention 108 + Convention for the protection of individuals with regard to the processing of personal data, June 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
8. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, January 28, 1981, https://rm.coe.int/1680078b37.

9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
10. Dülger, Murat Volkan. *Kişisel Verilerin Korunması Hukuku [Personal Data Protection Law]* (Hukuk Akademisi Yayınları, 2019).
11. European Data Protection Board. "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", European Data Protection Board, adopted on 07 July 2021, accessed September 5, 2024, https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.
12. Eren, Fikret. *Borçlar Hukuku Genel Hükümler [General Provisions of Law of Obligations]*. Yetkin Yayınları, 2018.
13. Fischer, Cyril. "Re-thinking the allocation of roles under the GDPR in the context of cloud computing", *International Data Privacy Law* 14, no.4 (2024): 53-65, https://doi.org/10.1093/idpl/ipad023.
14. Gauch, Peter, Walter R. Schluep, Jörg Schmid, Heinz Rey and Susan Emmenegger, *Schweizerisches Obligationenrecht [Swiss law of obligations], Allgemeiner Teil*, Schulthess, 2008.
15. Globocnik, Jure."On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID Directive 95/46/EC, Arts. 2(d) and (h), 7(a) and (f), 10", *International Review of Intellectual Property and Competition Law*, no.50 (2019): 1033-1044, https://doi.org/10.1007/s40319-019-00871-4.
16. Hess, Stephan. "The GDPR: Joint Controllership And Independent Controllership Should the SWIFT criteria determine the difference?." Thesis, Tilburg University, 2019.
17. Huguenin, Claire. *Obligationenrecht [Law of obligations], Allgemeiner Teil*, Schulthess, 2006.
18. Kaya, İrem. *KVKK ve GDPR Kapsamında Ortak Veri Sorumluluğu [Joint Data Controllership under KVKK and GDPR]*. On İki Levha Yayıncılık, 2023.
19. Kuner, Christopher. *European Data Protection Law: Corporate Regulation and Compliance*. Oxford University Press, 2007.
20. Küzeci, Elif. Kişisel Verilerin Korunması [Protection of Personal Data] (On İki Levha Yayıncılık, 2020).
21. Macmillan, Mac. "Data Protection Concepts", in *European Data Protection Law and Practice*, edited by Eduardo Ustaran. Iapp Publication, 2018.
22. Mäkinen, Jenna. "Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things", I*nformation & Communications Technology Law* 24, no.3 (2015): 262-277, http://dx.doi.org/10.1080/13600834.2015.1091128.
23. Oftinger, Karl, and Emil W. Stark, *Schweizerisches Haftpflichtrecht [Swiss liability law], Erster Band: Allgemeiner Teil.* Schulthess Polygraphischer Verlag, 1995.
24. Rey, Heinz. *Ausservertragliches Haftpflichtrecht [Non-contractual liability law]*, Schulthess, 2008.
25. Stalla-Bourdillon, Sophie, Henry Pearce and Niko Tsakalakis, "The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify", *Computer Law & Security Review* 34, no.4 (2018): 784-805, https://doi.org/ 10.1016/j.clsr.2018.05.012.

26. Van Alsenoy, Brendan. “Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation” JIPITEC 7, no.3 (2016): 271- 288, https://www.jipitec.eu/archive/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf.
27. Welfare, Damien and Peter Carey, “Territorial Scope and Terminology” in *Data Protection a Practical Guide to UK and EU Law*, edited by Peter Carey, Oxford University Press, 2018.
28. Wiedemann, Klaus, “Profiling and (automated) decision-making under the GDPR: A two-step approach”, *Computer Law & Security Review*, no. 45 (2022): 1-17, https://doi.org/10.1016/j.clsr.2022.105662.
29. Wong, Benjamin. “Problems With Controller-Based Responsibility in EU Data Protection Law”, *International Data Privacy Law*, Volume 11, Issue 4, (2021): 375–387, https://doi.org/10.1093/idpl/ipab014.
30. Zalnieriute, Monika and Genna Churches, “When a ‘Like’ Is Not a ‘Like’: A New FragmentedApproach to Data Controllership”, *The Modern Law Review* 84, no.4 (2020): 861- 876, doi: 10.1111/1468-2230.12537.