İSTANBUL UNIVERSITY PRESS

Annales de la Faculté de Droit d'Istanbul, 67: 125–140

DOI: 10.26650/annales.2018.67.0008
http://dergipark.gov.tr/iuafdi

Submitted: 01.10.2019
Accepted: 16.10.2019

Annales de la Faculté de Droit d'Istanbul

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Processing Data Made Public by the Data Subject under Swiss, European Union and Turkish Laws

İsviçre, Avrupa Birliği ve Türk Hukuklarına Göre İlgili Kişi Tarafından Kamuya Sunulmuş Verinin İşlenmesi

Nafiye Yucedag[1]

Abstract

The Law on the Protection of Personal Data numbered 6698 which was accepted on 24 March 2016 and was published on the Official Gazette dated 7 April 2016 and numbered 2967 is an adoption of the 95/46/EC Directive. The 95/46/EC Directive was repealed by the 2016/679/EU General Data Protection Regulation. However both regulations provide similar rules in regard to the processing of data made public by the data subject. In the Law on the Protection of Personal Data some provisions related to general justification grounds, one of which is the data made public by the data subject, differ with respect to those under European Union Law. In this study, the regulation on making data public by the data subject as a ground of justification has been evaluated in line with the aim of the Law on the Protection of Personal Data. In addition, European Union and Swiss Laws have been examined from a comparative perspective in order to shed light on the interpretation of the Law on the Protection of Personal Data.

Keywords

Personal data, Justification grounds, Making data public

Öz

24 Mart 2016 tarihinde kabul edilmiş ve 7 Nisan 2016 gün ve 29677 sayılı Resmi Gazete yayımlanmış olan 6698 sayılı Kişisel Verilerin Korunması Kanunu, temelde, 95/46/AT sayılı Yönerge'yi esas almıştır. 95/46/AT sayılı Yönerge ise, 2016/679/AB sayılı Tüzük ile yürürlükten kaldırılmıştır. Bununla birlikte her iki düzenleme ilgili kişi tarafından alenileştirilmiş kişisel verilerin işlenmesine ilişkin benzer kurallar getirmektedir. Öte yandan, ilgili kişinin kendisi tarafından kişisel verilerin alenileştirilmiş olması da dâhil olmak üzere genel hukuka uygunluk sebepleri açısından, Kanun'da, Yönerge'den farklı düzenlenmiş hususlar da bulunmaktadır. Bu çalışmada kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmesi hukuka uygunluk sebebi, Kanun'un amacına uygun olarak değerlendirilmiştir. Ayrıca, Avrupa Birliği ve İsviçre Hukuku düzenlemeleri karşılaştırmalı olarak Kişisel Verilerin Korunması Kanunu'nun uygulanmasına yol gösterici olması için incelenmiştir.

Anahtar Kelimeler

Kişisel veri, Hukuka uygunluk sebepleri, Alenileştirme

1 **Corresponding Author:** Nafiye Yucedag, (Res. Asst. Dr.) Istanbul University Faculty of Law, Department of Civil Law, Istanbul, Turkey. E-mail: nyucedag@istanbul.edu.tr ORCID: 0000-0002-5526-0323

To cite this article: Yucedag, Nafiye: "Processing Data Made Public by the Data Subject under Swiss, European Union and Turkish Laws", Annales de la Faculté de Droit d'Istanbul, 67, 2018, 125-140. https://doi.org/10.26650/annales.2018.67.0008

Processing Data Made Public by the Data Subject under Swiss, European Union and Turkish Laws

I. Introduction

The Law on the Protection of Personal Data[1] which was accepted on 24 March 2016 and which was published on the Official Gazette dated 7 April 2016 and numbered 2967 is an adoption of the 95/46/EC Directive[2]. The 95/46/EC Directive was repealed by Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC[3]. However, some provisions in the Turkish Data Protection Code differ with respect to those under the 95/46/EC Directive and GDPR. Making data public as a justification ground has been regulated under the Law on the Protection of Personal Data and is considerably different from the 95/46/EC Directive Art. 8(2)(e) and GDPR Art. 9(2)(e). According to LPPD Art. 5(2)(d) personal data may be processed without seeking the explicit consent of the data subject if the data concerned is made available to the public by the data subject himself. Swiss Federal Act on Data Protection Art. 12(3) and Law on the Protection of Personal Data Art. 5(2)(d) share considerable similarities compared to GDPR Art. 9(2)(e). GDPR Art. 9(2)(e) does not only require data to be sensitive but also requires that sensitive data should be manifestly made public. Therefore, a comparative analysis with Swiss Law in addition to European Union Law has also been conducted in order to shed light on the interpretation of the Law on the Protection of Personal Data Art. 5(2)(d).

II. Processing Data Made Accessible to the Public by the Data Subject under Swiss Law

A. In General

According to the Swiss Federal Act on Data Protection[4] Art. 12(3): "*As a rule there is no breach of personality rights if the data subject has made the data generally accessible and has not expressly prohibited its processing*." Under Swiss Law then, processing data which has been made generally accessible by the data subject is in

1 Law on the Protection of Personal Data numbered 6698 published on the Official Gazette dated on 7 April 2016 and numbered 2967 (hereafter "LPPD").

2 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 (hereafter "95/46/EC Directive").

3 Regulation 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR").

4 Bundesgesetz über den Datenschutz numbered 235 (hereafter "DSG").

principle not considered to be breaching the privacy of the data subject. The law-maker has accepted a legal presumption (by stating that "*as a rule" "in der Regel*") that can be refuted[5].

B. Making Data Generally Accessible

First, under DSG Art. 12(3) the data should be made publicly accessible. Data is made generally accessible to the public when an indeterminate number of people has access to it without any significant obstacle[6]. It is required that the data subject takes all necessary steps to make the data publicly accessible. Even if the data is not eventually announced to the public, the requirement of making it publicly accessible under DSG Art. 12(3) would be met[7]. If the data subject has made a press release and the article that quotes the data subject is not published, it will be accepted that the data is made accessible to the public under the terms of Art. 12(3)[8].

The data subject should knowingly and willing make the data accessible to the public. If the data is published on a public register without the data subject's will and knowledge, DSG Art. 12(3) will not be applicable. Similarly, personal data that must be published because of a legal obligation is not covered by DSG Art. 12(3)[9].

The data subject is actually not obliged to make the data accessible to the public themselves. A third party can make the data publicly accessible provided that he/she has acted with the knowledge and will of the data subject. This would be the case if the data subject is registered in a public directory (for instance the telephone directory)[10].

It is also important to evaluate a person's actions in the public space. In public spaces, a person's appearance and behaviour might be observed by others. However, in many cases the data subject will not be determinable and therefore data protection concerns will not be raised. Even when it is possible to determine the data subject, he/she would not be making his/her data publicly accessible willingly and knowingly by appearing in public spaces. Being in a public space would not necessarily result in making the data accessible to the public since the data subject would assume that

5 **David Rosenthal/ Yvonne Jöhri**, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Schulthess Juristische Medien AG, 2008,, Art. 12, Nr. 50; **Corrado Rampini,** Basler Kommentar, Datenschutzgesetz, ed. Vogt Nedim Peter/Maurer-Lambrou Urs, 3. Auflage, Basel, 2014, Art. 12, Nr. 18; Bundesverwaltungsgericht, Decision Nr. A-3144/2008 dated 27.5.2009, Nr. 9.3.5; but see **Marc, Wullschleger**, "Die Durchsetzung des Urheberrechts im Internet, SMI - Schriften zum Medien- und Immaterialgüterrecht" Band/Nr. 101, 2015, pp. 28-58, Nr. 82.

6 **Rosenthal/Jöhri**, Art. 12, Nr. 54; **Wullschleger**, Nr. 84; **Nafiye Yücedağ**, **"**The Protection Of IP Addresses In Peer-To-Peer (P2P) Networks", 13th International Conference on Internet, Law & Politics "Managing Risk in the Digital Society", Huygens Editorial, Barselona, 2017, p. 349.

7 **Rosenthal/Jöhri**, Art. 12, Nr. 54 and 63.

8 **Rosenthal/Jöhri**, Art. 12, Nr. 63.

9 **Wullschleger**, Nr. 84.

10 **Rosenthal/Jöhri**, Art. 12, Nr. 55.

passers-by or travellers in public transport would have no interest in taking his/her picture, following his/her consumption habits or listening to his/her telephone conversations[11].

Similarly, if the data subject was photographed by a hidden or overt camera, but was not in a position to assume unambiguously that the images would be made accessible to the public, any publication would not only be done without the knowledge of the data subject, but also without their will. If a person attends a party where journalists are also invited, he/she should assume that the pictures taken at that event will be published. On the other hand, publishing photographs of a private funeral without the consent of the mourners, even if the ceremony takes place in a public place, would not be considered lawful processing under DSG Art. 12(3)[12].

If the data subject knows that personal data are to be made generally accessible (for instance in the form of a newspaper report) and the data subject remains passive, DSG Art. 12 (3) will not be applicable. However, the fact that processing of personal data has been tolerated may be of some relevance in the context of justification on the basis of an overweighting private or public interest[13].

In the event of a dispute, the data controller must prove not only that he obtained the personal data from a publicly accessible source, but also that the data in question, with the knowledge and will of the data subject, was made accessible to the public. This will often be difficult for the data controller, especially when the data is not directly obtained from the data subject[14]. The data controller must also prove that all personal data has been made generally accessible to the public by the data subject. If the personal data made accessible to the public is supplemented by further data which is not made accessible to the public, the data controller cannot base their claim on the presumption provided under DSG 12(3) for the processing of this further data. On the other hand, the data controller can use personal data that the data subject has made publicly accessible on various media (for instance citations from various interviews, supplemented with images from the data subject's website) and combine them[15].

C. No Prohibition on Processing

The presumption under DSG Art. 12(3) provides that once the data has been made accessible to the public by the data subject, there is no breach of privacy. In order to apply this presumption however, the data subject should not have expressly prohibited the processing. By prohibiting the processing, the data subject regains control of

11 see. **Rosenthal/Jöhri**, Art. 12, Nr. 57.

12 **Rosenthal/Jöhri**, Art. 12, Nr. 59.

13 **Rosenthal/Jöhri**, Art. 12, Nr. 56.

14 **Rosenthal/Jöhri**, Art. 12, Nr. 64.

15 **Rosenthal/Jöhri**, Art. 12, Nr. 65.

publicly accessible personal data[16]. This also means that processing is possible until the data subject declares a prohibition. Under certain circumstances, personal data that has been made accessible to the public can be transferred by a third party, without this third party being aware of any prohibition. In practice, this leads to difficulties, especially when personal data is on the internet, which for instance can be the case for vacation photos, which may be accessible worldwide by anyone. In practice, the data subject will be almost unable to prohibit the subsequent processing by third parties as soon as the personal data has become generally accessible on the internet[17].

The express prohibition applies only for the addressee. In accordance with the general rules of the Code of Obligations, a declaration of will can only have an effect if it is addressed to and received by a data controller[18]. The data subject may prohibit a particular newspaper from using photographs which previously were made public[19], but the prohibition of processing should reach the addressee. Pop-ups, in this respect, might not be an effective means because pop-up blockers might be in place[20]. In order to interpret a declaration of prohibition, the general provisions of the Code of Obligations on declarations of will must also be taken into account. If the prohibition is provided through an agreement, the general provisions of the Code will be applicable to the validity of this clause. The clause, therefore, might be characterized as an unfair contractual term[21].

D. The Presumed Public Availability Aim of the Data Subject

The presumption, nonetheless, can be rebutted even when the data subject has made the data generally accessible to the public and has not prohibited its processing. In this context, an objective assessment can be conducted by taking into account the understanding of a reasonable data controller. What should be evaluated is whether the data controller has processed the data in the same way and with the same aim as the data subject in the concrete circumstances of the case[22]. Data controllers can

16 **Wullschleger**, Nr. 91.

17 **Wullschleger**, Nr. 91.

18 **Wullschleger**, Nr. 92.

19 **Rosenthal/Jöhri**, Art. 12, Nr. 67.

20 **Rosenthal/Jöhri**, Art. 12, Nr. 70.

21 **Rosenthal/Jöhri**, Art. 12, Nr. 71.

22 See **Rosenthal/Jöhri**, Art. 12, Nr. 75; **BSK DSG/Rampini**, Art. 12, Nr. 18; **Yücedağ**, The Protection of IP Addresses in Peer-To-Peer (P2P) Networks, p. 349. European Court of Human Rights in its decisions has taken into account the reasonable expectation criterion in relation to the protection of private life in a public space, which might seem to be a similar limitation to the obvious publication aim of the data subject under Swiss Law. According to the ECHR "*There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain*" (P.G. and J.H. v. the United Kingdom, Case No. 44787/98, Para. 57). In the Peck v. United Kingdom

process the data made generally accessible subject to the obvious public accessibility aim of the data subject (*ersichtlichen Veröffentlichungszwecks*)[23].

For instance, an e-mail address made available by the data subject on a website does not mean that he/she agrees to receiving spam mail[24]. Similarly, if a newspaper publishes the image of a singer whose dress has accidentally slipped during a performance so that part of her breast became visible, such a processing would be viewed as running against the public availability aim of the data subject[25]. However, if a newspaper publishes the image of a speaker at an event, such processing would be viewed as in line with the public availability aim of the data subject[26]. This criterion would also prevent misuse of data on the internet.

According to another view, it cannot be excluded that the presumed aim of the data subject is not supported by the text of Art. DSG 12(3)[27]. *Wullschleger* states that the unwritten criterion of the presumed aim is problematic if the informational right to self-determination is taken seriously, since under DSG Article 12(3) the processing of publicly accessible data is permitted until processing is expressly prohibited[28].

If the data is processed against the presumed will of the data subject by breaching his/her privacy, DSG Art. 12(3) will not be applicable. However, even if the presumption under DSG Art. 12(3) is refuted, the data controller may rely on the justification grounds of Art. 13. According to Art. 13(1), a breach of personality rights is unlawful unless it is justified by an overriding private or public interest or by law. Art. 13 (2) mentions various reasons for justification, and this list is not exhaustive. While balancing the interest of the data subject with a private or public interest, data that has been made accessible to the public can be taken into account. It might be said that if the data has never been made accessible to the public, the threshold for the assessment of the breach of personality rights will be higher. There will be a reduction of the interest attached to the protection against personality rights breach

case, the Court also used the reasonable expectation test. The applicant had attempted suicide by cutting his wrists and the immediate aftermath of the incident was recorded. The footage and photos of the applicant were then released on many audio-visual media. The court decided that "*the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation (...) and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995*" (Peck v. The United Kingdom, Case No. 44647/98, Para. 62). A reasonable person under the same circumstances as Mr. Peck would not foresee that the data would have been used and disclosed in such a manner (**Tomás Gómez-Arostegui**, "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations", California Western International Law Journal, Vol. 35 (2005) No. 2, p. 171) see also Perry v. United Kingdom, Case No. 63737/00, Para. 40 et seq.

23 **BSK DSG/Rampini**, Art. 12, Nr. 18; Bundesverwaltungsgericht, Case Nr. A-3144/2008 dated 27.5.2009, Para. 9.3.5.

24 **BSK DSG/Rampini**, Art. 12, Nr. 18; **Amédéo Wermelinger**, Datenschutzgesetz, ed. Bruno Baeriswyl/ Kurt Pärli, Stämpflis Handkommentar, 2015, Art. 12, Nr. 11.

25 **Rosenthal/Jöhri**, Art. 12, Nr. 77.

26 **Rosenthal/Jöhri**, Art. 12, Nr. 78.

27 **Wullschleger**, Nr. 86.

28 **Wullschleger**, Nr. 86.

when the data subject makes the data available to the public[29]. It can be also accepted that, in such cases, the threshold for considering that a public or private interest is overriding might be reduced as well[30].

III. Processing Data Made Manifestly Public by the Data Subject under European Union Law

Personal data is defined under 95/46/EC Directive as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". Personal data might be categorized either as sensitive data or as data other than the sensitive data. According to Article 8(2)(e) of the 95/46/EC Directive, data relating to "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life" are considered to be "special categories" of data or in other words, sensitive data.

The protection grounds for sensitive data are regulated under Art. 8 of the 95/46/EC Directive. 95/46/EC Directive Art. 8(2)(e) states that processing data which is manifestly made public by the data subject is not prohibited. The General Data Protection Regulation similarly provides in Art. 9(2)(e) that the processing of sensitive data which is manifestly made public by the data subject is not prohibited.

A. Application of General Justification Grounds to Data Made Public by the Data Subject

95/46/EC Directive Art. 7 regulates the criteria for making data processing legitimate, which would apply at least to the processing of non-sensitive data. However, it is questionable whether only the justification grounds mentioned under 95/46/EC Directive Art. 8 would be sufficient to consider the processing of sensitive data lawful. 95/46/EC Directive Art. 8 prohibits the processing of sensitive data with exceptions. These exceptions may however be regarded as requirements that limit the scope of the prohibition. Nonetheless, these requirements do not *per se* constitute a legitimate justification ground for the processing in all cases[31]. The Working Party in its opinion numbered 06/2014 considered that "*an analysis has to be made on a case by case basis whether 95/46/EC Directive Art. 8 in itself provides for stricter and sufficient conditions*"[32].

29 **Rosenthal/Jöhri**, Art. 12, Nr. 80; **Yücedağ**, The Protection of IP Addresses in Peer-To-Peer (P2P) Networks, p. 349 - 350.

30 **Rosenthal/Jöhri**, Art. 12, Nr. 81.

31 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 15, fn. 30; See also **Nilgün Başalp,** Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004, p. 45.

32 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 15.

95/46/EC Directive Art. 8(2)(e) states that processing data which is manifestly made public by the data subject is not prohibited. However, this justification ground regulates only the processing of sensitive data. It is questionable whether once data is made publicly available by its subject, its processing will be considered lawful. The data which is sensitive, once made public by the data subject, is still personal data. Thus, personal data which is not sensitive cannot be processed even if it is manifestly made public by the data subject, since 95/46/EC Directive Art. 7 does not provide for such a justification ground[33]. In order to justify the processing of such data, one of the justification grounds of Article 7 must exist. Therefore, if sensitive data which is made available to the public is processed, one of the justification grounds under Article 7 will be met *a fortiori*. In this context, data made manifestly public under Article 8 (2)(e) will not always result in making the processing of such data lawful. In most of these cases, a balancing of interest under Art. 7(f) will be necessary[34].

The General Data Protection Regulation similarly regulates under Art. 9(2)(e) that processing sensitive data which is manifestly made public by the data subject is not prohibited. However, it is not enough for the personal data to be publicly accessible. Making data available to the public must be the result of a deliberate act of the data subject[35]. A data subject who expressly makes their data available to the public waives their right to the special protection provided under GDPR Art. 9. However, the general protection provisions under GDPR Art. 6 will remain applicable[36]. In this case, the legislature considers that there is no particular need for protection of the data made public, so that the lawfulness of the processing is governed solely by the general grounds provided under Article 6 (1)[37].

B. Data Manifestly Made Public

The term 'making public' is defined neither under 95/46/EC Directive nor under the GDPR. It is generally accepted that the data is made available to the public when an indeterminate number of people has access to it without any significant obstacle[38]. On social networks, whether or not the data is made available to the public will depend

33 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 15, fn. 31.

34 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 15.

35 **Thomas Petri**, Datenschutzrecht, DSGVO mit BDSG, ed. Spiros Simitis/ Geritt Hornung/Indra Spiecker gen. Döhmann, Datenschutzrecht, DSGVO mit BDSG, Nomos Verlag, 2019, Art. 9, Nr. 57.

36 **Thilo Weichert**, Datenschutz-Grundverordnung Kommentar, ed. Jürgen Kühling/Benedikt Buchner, 2. Auflage, München 2018, Art. 9, Nr. 77.

37 **Sebastian Schulz**, DS-GVO – Datenschutzgrundverordnung VO (EU) 2016/679 – Kommentar, ed. Peter, Gola, 2. Aufl. 2018, Art. 9, Nr. 25; **Marion Albers/ Raoul-Darius Veit,** Beck'scher Online-Kommentar Datenschutzrecht, 29. edition, Heinrich Amadeus Wolff/Stefan Brink, München, 2018, Art. 9, Nr. 63 and 64; Simitis/Hornung/Spiecker/Petri, Art. 9, Nr. 57.

38 **Gola DS-GVO/Schulz DS-GVO**, Art. 9, Nr. 26; **BeckOK DatenschutzR/Albers/Veit DS-GVO,** Art. 9, Nr. 65; **David Kampert**, Europäische Datenschutzgrundverordnung, ed. Gernot Sydow, 2. Auflage, Nomos Verlagsgesellschaft, 2018, Art.9, Nr. 31.

on those data being available to the general public or only within closed groups or circles[39], according to the privacy settings chosen by the data subject. However, because of the amount of the friends with whom the data has been shared and because it is not always manageable for the data subject, the data should be accepted as made available to the public[40]. Similarly, if anyone can become a member of a network, the data made available to all users of that network even if the number of people is determinable at the time of making data available[41]. It is necessary to assess the recipient radius according to the understanding of the data subject at the time the data is made available. In cases where the data subject could not have expected that, in the foreseeable future, the number of recipients would grow to an unmanageable level, the data should not be considered as having been made available to the public. This could happen where the accessibility status of a closed group has changed in time[42].

The term 'manifestly' is intended to prevent a data subject losing the special protection provided under Art. 9(2)(e) in cases where a third party discloses the sensitive data to the public. Therefore, not all publicly available data will fall under Art. 9(2)(e), as the mere fact that data is publicly available is not sufficient to forego the protection provided under Art. 9. The public availability of the data must obviously be the result of the will of the data subject[43]. This is not the case, for instance, if the public availability of the data is based on an administrative or judicial decision without the consent of the data subject[44].

Furthermore, a mere tolerance of the processing by the data subject will not usually suffice[45]. In the case of public profiles on social networks, the personal data provided will be considered as available to the public[46].

If the data controller, through profiling, derives sensitive personal data from non-sensitive personal data that the data subject has made public, that sensitive personal data is therefore typically not manifestly made public. The opposite outcome would hardly be consistent with the principle of good faith under GDPR Art. 5 (1)(a)[47].

In order to assess whether the data is made available to the public, the understanding of an objective external observer should be taken into account[48]. If the data controller,

39 **Gola DS-GVO/Schulz DS-GVO**, Art. 9, Nr. 26.

40 **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 78.

41 See **Simitis/Hornung/Spiecker/Petri**, Art. 9, Nr. 58.

42 See **Gerald Spindler/ Lukas Dalby**, Recht der elektronischen Medien, ed. Gerald Spindler/ Fabian Schuster, 4. Auflage, Verlag C.H. Beck, München, 2019, Art. 9, Nr. 14

43 **Sydow/Kempert**, Art.9, Nr. 32.

44 **Sydow/Kempert**, Art.9, Nr. 32.

45 **Simitis/Hornung/Spiecker/Petri**, Art. 9, Nr. 59.

46 **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 79.

47 **Simitis/Hornung/Spiecker/Petri**, Art. 9, Nr. 61.

48 See **Simitis/Hornung/Spiecker/Petri**, Art. 9, Nr. 59; **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 80; **BeckOK DatenschutzR/Albers/Veit DS-GVO**, Art. 9, Nr. 66.

or a reasonable person in the position of the data controller, has an understanding that the data is made available to the public, even if the understanding of the data subject contradicts it, the data should be accepted as having been made publicly available. In cases of uncertainty as to whether the data has been made available by the data subject, this justification ground will not be applicable[49].

For instance, in most cases it will be doubtful that data found in internet and press publications has been made public by the data subject[50]. The same applies to press releases, unless it is clear that the information comes from the data subject, for instance through the use of authorized quotations[51].

Websites accessible only to a limited number of friends should not be considered as public[52]. Personal data provided on the websites of persons other than the data subject is not manifestly made public, unless the consent of the data subject is apparent from the circumstances. Information accessible via a search engine cannot lead to the conclusion that this data has been made available to the public by the data subject[53]. In cases of a personal blog or publicly accessible member messages with the name of the data subject or telephone directories in which one can register voluntarily, the data can be assumed to be made available to the public by the data subject[54].

The mere presence of sensitive data in public spaces is not sufficient to make data available to the public[55]. Therefore, participation in a public event does not legitimize the processing of sensitive data (for instance media reports or photographs about this event) obtained because of this participation[56]. Making certain data accessible to an indeterminate group of people cannot be equated with moving in a public space[57].

IV. Processing Data Made Available to the Public by the Data Subject under Turkish Law

According to the Law on the Protection of Personal Data Art. 5(2)(d) personal data may be processed without seeking the explicit consent of the data subject if the data concerned is made available to the public by the data subject himself. For this purpose, according to the Turkish Data Protection Authority, making data available to

49 See **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 80.

50 **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 80.

51 **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 82.

52 **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 82.

53 **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 82.

54 **Kühling/Buchner/Weichert DS-GVO**, Art. 9, Nr. 81.

55 **BeckOK DatenschutzR/Albers/Veit DS-GVO**, Art. 9, Nr. 66; **Alexander Schiff,** DSGVO Datenschutz - Grundverordnung Kommentar Eugen Ehmann/ Martin Selmayr, C.H. Beck, 2018, Art. 9, Nr. 46.

56 **BeckOK DatenschutzR/Albers/Veit DS-GVO**, Art. 9, Nr. 66.

57 **Ehmann/Selmayr/Schiff DS-GVO**, Art. 9, Nr. 46.

the public means making data knowable by everyone[58]. For instance, the publication of employees' corporate telephone numbers and e-mail addresses on corporate websites makes this data available to the public[59].

As explained above, processing data made publicly available by the data subject is considered to be lawful under Swiss Law and European Union Law only if certain conditions have been met. Art. 12(3) of the Swiss Federal Act on Data Protection and Art. 5(2)(d) of the Law on the Protection of Personal Data share considerable similarities compared to Art. 9(2)(e) of the GDPR. Unlike GDPR Art. 9(2)(e), these two rules are not applicable to sensitive data and require data to be publicly accessible. In this regard, GDPR Art. 9(2)(e) does not only require data to be sensitive, but also that this sensitive data should be manifestly made public. This term manifestly raises the threshold for the application of the article and prevents the data subject from losing the special protection provided under GDPR Art. 9(2)(e) under strict conditions. Considering that GDPR Art. 9(2)(e) is applicable to sensitive data, the application of a high threshold can be deemed necessary.

In the General Preamble of the Law on the Protection of Personal Data, it is stated that there is no worthy legal protection in the processing of the data made available to the public by the data subject[60]. However, this assumption stated in the Preamble will not be valid in all cases. Moreover, this assumption is not in line with the personal data protection aim and European Union Law. According to GDPR Art. 9(2)(e) once the data has been made manifestly available to the public, the data subject waives his/her right only to special protection provided under GDPR Art. 9. However, the data subject is not left without any protection since the justification grounds under Art. 6 will still be applicable. The fact that the data has been made publicly available by the data subject will not make its processing lawful for any purpose and in any manner.

In this regard, LPPD Art. 5(2)(d) should be interpreted narrowly according to the purpose of the Law. Even when data has been made available to the public by the data subject, it should not be possible to deem the processing to be lawful if the data has not been processed in line with the publication aim in the concrete circumstances of

58 Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kanun'da Yer Alan Terimler, p. 9 (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7452edd6-9ce1-4988-9cfc-95b3758fbd1b.pdf, last online access 15.10.2019)

59 **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi, p. 44. (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf, last online access 15.10.2019), s. 76.

60 LPPD, General Preamble, p. 20; Similarly **Furkan Güven Taştan,** Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul, 2017, p. 172. According to *Aydın* making data available to public would mean an implicit consent. (**Sedat Erdem Aydın**, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, On İki Levha Yayıncılık, İstanbul, 2015, p. 147). According to our opinion in this case there is no implicit consent. If one would have to refer to consent, it could only be a presumed consent. See also Turkish Court of Appeals, 12. Criminal Chamber, File No. 2014/4081, Decision No. 2014/19490 (Kazancı Elektronik Hukuk Yayımcılığı, last online access 15.10.2019).

the case[61]. The data controller has to process the data in the same way and with the same aim as the data subject could reasonably expect him to.

The Turkish Data Protection Authority also stated that personal data should not be used beyond the purpose of publication. For instance, it is not possible to use for marketing purposes the contact information of a data subject who has provided his/her contact information in order to sell his/her vehicle through a website where second-hand vehicles are sold[62]. Similarly, if, for the evaluation of an application for a job, an employer checks the profiles of the candidates on various social networks and includes information from these networks that is not related to the business life of the data subject, the data processing would fall beyond the publication aim of the data to the public. However, processing can be considered to be lawful under LPPD Art. 5 (2)(f), if the processing of the data available on the social media networks is necessary to assess specific risks regarding candidates for a specific function and the candidates are well informed[63].

According to LPPD Art. 28 (2)(b) "*Provided that it is in compliance with and proportionate to the purpose and fundamental principles of this Law, Article 10 regarding the data controller's obligation to inform, Article 11 regarding the rights of the data subject, excluding the right to demand compensation, and Article 16 regarding the requirement of enrolling in the Registry of Data Controllers shall not be applied*" where personal data processing is carried out on the data which is made public by the data subject himself/herself. According to this provision, the rights of the data subject, excluding the right to demand compensation, cannot be remedied. In this regard, the Law on the Protection of Personal Data will in part not be applicable to the data made available to the public by the data subject. For instance, if a person shares personal data in a publicly accessible way on a social media network, the processing of such data will be covered by Turkish Data Protection Law only in part[64].

If the data subject made the data publicly available, he/she can to demand compensation but will not be able to learn whether his/her personal data are processed or not, to request information if his/her personal data are processed, to learn the purpose of his/her data processing and whether this data is used for intended

61 **Nafiye Yücedağ**, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Nr.75, Y. 2018, p. 781; See also **Şehriban İpek Aşıkoğlu**, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi No:5, On İki Levha Yayıncılık, İstanbul, 2018, p. 131. According to differing opinion processing has to in line with the general principles under KVKK Art. 4 (**Elif Küzeci**, Kişisel Verilerin Korunması, Turhan Kitapevi, Ankara, 2019, p. 346; **Murat Volkan Dülger**, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yayıncılık, İstanbul, 2019,p. 326). In this regard processing public data by data controller data has to be in line with the publication purpose of the data subject. This opinion derives the purpose limitation based on the principle of data minimization.

62 **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi, p. 76.

63 **Article 29 Data Protection Working Party,** Opinion 2/2017 on data processing at work, p. 11.

64 **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi, p. 44.

purposes, to know the third parties to whom his/her personal data is transferred at home or abroad, to request the rectification of the incomplete or inaccurate data, if any, and to request the erasure or destruction of his/her personal data under the conditions laid down in Article 7. In addition, he/she will not be able to object to the processing, exclusively by automatic means, of his/her personal data, which leads to an unfavourable consequence for him/her.

This provision can be criticized in two respects. First of all, the act must be unlawful in order for compensation for the damages caused by the act to be awarded, according to the rules of tort law. As a rule, then, there will be no liability for an act unless it is an unlawful act (TCO Art. 49). However, although an act is deemed to be lawful, it is possible liability for damages to arise. For example, in case of necessity, a person who damages the property of another in order to protect himself/herself or another person against imminent damage or danger must pay damages [TCO Art. 64 (2)]. The victim must bear this loss and, in return, the offender must make a sacrifice by compensating the damage to the extent that equity requires (the principle of balancing of sacrifices)[65].

In our opinion, the legislator did not intend to provide a legal basis for balancing of sacrifices if the act is in accordance with the law. The processing of personal data made public by the data subject is either lawful or unlawful. If the processing of data made public by the data subject is lawful, there would be no reason for the data controller to enact a sacrifice in order to compensate for the damages. Secondly, it may be vital for the data subjects to exercise their rights, other than the right to compensation, provided under LPPD Art. 11. In particular, data subjects will have an interest in learning whether their personal data are processed or not, requesting information if their personal data are processed, learning the purpose of their data processing and whether this data is used for intended purposes, knowing the third parties to whom their personal data is transferred at home or abroad, requesting the rectification of the incomplete or inaccurate data, if there is any, and in requesting the erasure or destruction of their personal data. In our opinion taking away these rights from the data subject is not appropriate[66].

V. Conclusion

According to LPPD Art. 5(2)(d) personal data may be processed if the data concerned is made available to the public by the data subject. Similarly, according to Swiss Federal Act on Data Protection Art. 12(3); "*As a rule there is no breach of personality rights if the data subject has made the data generally accessible and*

65 **İlhan Ulusan**, Medeni Hukukta Fedakârlığın Denkleştirilmesi İlkesi ve Uygulama Alanı, 2. Bası, Vedat Kitapçılık, İstanbul, 2012, p. 99 et seq.

66 **Yücedağ**, Medeni Hukuk Açısından, p.781.

has not expressly prohibited its processing". The data made available to the public means that an indeterminate number of people has access to it without any significant obstacle. For instance, on corporate websites, publication of employees' corporate telephone numbers and e-mail addresses means data has been made available to the public. In this regard under Swiss Law it is widely accepted that the data made available to the public by the data subject shall be processed in line with the publication aim of the data subject in the concrete circumstances of the case.

According to GDPR Art. 9(2)(e) once the data has been made manifestly available to the public, the data subject waives his/her right only to special protection provided under GDPR Art. 9. However, the data subject is not left without any protection since the justification grounds under Art. 6 will still be applicable. Therefore, processing data made public by the data subject will be subject to a twofold test under European Union Law.

Even if the wording of LPPD Art. 5(2)(d) does not require any limitation on the processing of the data made public, as in the case of DSG Art. 12(3), taking into account the aim of the Law on the Protection of Personal Data, LPPD Art. 5(2)(d) should be interpreted narrowly. The data made available to the public by the data subject shall be processed in line with the publication aim of the data subject in the concrete circumstances of the case. Processing should not be deemed lawful unless another justification ground exists.

According to LPPD Art. 28(2)(b) the rights of the data subject, excluding the right to demand compensation, shall not be applied if the data was made available to the public by the data subject. According to our opinion the legislator does not intend to provide a legal basis, as a sacrifice for the data controller, for the compensation if the act is in accordance with the law. It may also be significantly important for the data subjects to exercise their rights, other than the right to compensation, provided under LPPD Art. 11. Therefore, LPPD Art. 5(2)(d) shall be strictly interpreted considering that the data subject cannot remedy the other rights apart from the right to compensation.

Grant Support: The author received no grant support for this work.

Bibliography

Albers Marion/ Veit Raoul-Darius, Beck'scher Online-Kommentar Datenschutzrecht, 29. Edition, Wolff, Heinrich Amadeus/Brink Stefan, München, 2018 ("BeckOK DatenschutzR/ Albers/Veit DS-GVO").

Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work.

Aşıkoğlu Şehriban İpek, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi No:5, On İki Levha Yayıncılık, İstanbul, 2018.

Başalp Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004.

Dülger Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yayıncılık, İstanbul, 2019.

Gómez-Arostegui, Tomás, "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations", California Western International Law Journal, Vol. 35 (2005) No. 2, pp. 153 – 202.

Kampert David, Europäische Datenschutzgrundverordnung, ed. Sydow Gernot, 2. Auflage, Nomos Verlagsgesellschaft, 2018 ("Sydow/Kampert").

Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kanunda Yer Alan Terimler, (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7452edd6-9ce1-4988-9cfc-95b3758fbd1b.pdf)

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi, (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf).

Küzeci Elif, Kişisel Verilerin Korunması, Turhan Kitapevi, Ankara, 2019.

Petri Thomas, Datenschutzrecht, DSGVO mit BDSG, ed. Simitis Spiros/Hornung Geritt/ Döhmann Indra Spiecker, Datenschutzrecht, DSGVO mit BDSG, Nomos Verlag, 2019 ("Simitis/Hornung/Spiecker/Petri").

Rampini Corrado, Basler Kommentar, Datenschutzgesetz, ed. Vogt Nedim Peter/Maurer-Lambrou Urs, 3. Auflage, Basel, 2014 ("BSK DSG/Rampini").

Rosenthal David / Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Schulthess Juristische Medien AG, 2008.

Schiff Alexander, DSGVO Datenschutz - Grundverordnung Kommentar Ehmann Eugen/Selmayr Martin, C.H. Beck, 2018 ("Ehmann/Selmayr/Schiff DS-GVO").

Schulz Sebastian, DS-GVO – Datenschutzgrundverordnung VO (EU) 2016/679 – Kommentar, ed.Gola, Peter, 2. Aufl. 2018 ("Gola DS-GVO/Schulz").

Sedat Erdem Aydın, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, On İki Levha Yayıncılık, İstanbul, 2015.

Spindler Gerald/Dalby Lukas, Recht der elektronischen Medien, ed. Spindler Gerald/Schuster Fabian, 4. Auflage, Verlag C.H. Beck, München, 2019 ("Spindler/Schuster Elektron. Medien/Spindler/Dalby DS-GVO").

Taştan Furkan Güven, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul, 2017.

Ulusan İlhan, Medeni Hukukta Fedakârlığın Denkleştirilmesi İlkesi ve Uygulama Alanı, 2. Bası, Vedat Kitapçılık, İstanbul, 2012.

Wermelinger Amédéo, Datenschutzgesetz, ed. Baeriswyl, Bruno / Pärli, Kurt, Stämpflis Handkommentar, 2015.

Weichert Thilo, Datenschutz-Grundverordnung Kommentar, ed. Kühling, Jürgen / Buchner, Benedikt , 2. Auflage, München 2018 ("Kühling/Buchner/Weichert DS-GVO").

Wullschleger Marc, Die Durchsetzung des Urheberrechts im Internet, SMI - Schriften zum Medien- und Immaterialgüterrecht Band/Nr. 101, Stämpfli Verlag AG, Bern, 2015.

Wermelinger Amédéo, Datenschutzgesetz, ed. Baeriswyl Bruno / Pärli Kurt, Stämpflis Handkommentar, 2015.

Yücedağ Nafiye, "The Protection of IP Addresses in Peer-To-Peer (P2P) Networks", 13th International Conference on Internet, Law & Politics "Managing Risk in the Digital Society", Huygens Editorial, 2017, pp. 342-357 (http://www.huygens.es/ebooks/IDP_2017.pdf) ("The Protection of IP Addresses in Peer-To-Peer (P2P) Networks").

Yücedağ, **Nafiye**, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Nr.75, Y. 2018, pp.765-789 ("Medeni Hukuk Açısından").