science editing
pISSN 2288-8063
eISSN 2288-7474
Sci Ed 2019;6(1):73-77
https://doi.org/10.6087/kcse.158

Essay

Personal data protection of academic journals in the age of the European General Data Protection Regulation: guidelines for Korean journals

Juyoen Lee[1], Eric Yong Joong Lee[2]

[1]Jinsol LLC, Seoul; [2]College of Law, Dongguk University, Seoul, Korea

Introduction

There are many publications addressing the General Data Protection Regulation (GDPR) of the European Union (EU), which came into force in May 2018. Many writers have acknowledged that Korean companies handling EU customers and their personal data are subject to the GDPR. These writers also explain the differences between the GDPR and Korea's Personal Information Protection Act (PIPA) [1,2] and how to cope with the GDPR [3,4]. The question is whether the GDPR affects Korea-based academic journals. Some readers may have ignored the GDPR, assuming that it has little bearing on academic journals, unlike business entities that trade personal data and companies whose success often depends on how much personal data they retain. Other readers, if they manage journals whose contributors or reviewers include EU citizens, might have wondered if they are subject to the GDPR as well.

What Does the GDPR Signify for Korean Journals?

Technically speaking, non-EU based journals, including Korea-based journals, cannot completely escape the GDPR, as the Regulation is applicable to all persons and entities—regardless of whether they are EU-based or not or they are acting for-profit or not—that process (e.g., collect, store, and use) the personal data of people who are in the EU for the purpose of offering goods or services [GDPR Art. 3(2)]. To be more specific, a non-EU based (e.g., Korean) journal that accepts the EU user registrations and subscriptions becomes a "data controller" according to Articles 3(2) and 4(7) of the GDPR. A data controller is a person or other body that determines the purposes of and means for processing personal data. Consequently, Korean journals must take the GDPR into account. As a result, the editor of a Korean journal should also be mindful of how the GDPR affects his or her journal's activities because the editor, under the direct authority of the journal [data controller], is authorized to process (e.g., retrieve or share with others, if necessary) personal data.

Received: November 26, 2018
Accepted: December 11, 2018

Correspondence to Eric Yong Joong Lee
grotian@dongguk.edu

ORCID
Juyoen Lee
https://orcid.org/0000-0002-0190-0030
Eric Yong Joong Lee
https://orcid.org/0000-0001-5640-490X

In addition, it is noteworthy that PIPA's definition of "data subjects" includes any living person, regardless of his or her nationality [5]. The PIPA Art. 2(5) provides for *gaeinjeongbocheorija*, defined as a public body, legal person, organization, individual, *et cetera*, that processes personal data for the performance of a task, which is equivalent to a data controller under the GDPR. Korean journals serve this function. The PIPA defines the term *gaeinjeongbocheorichwigeubja* (i.e., journal editor) as a person processing personal data under the command or supervision of the controller [PIPA Art. 28(1)]. In other words, Korean journals and their editors assumed the duty of protecting the personal data of European citizens under the terms of the PIPA before the GDPR came into force. This means that the enforcement of the GDPR will not require meaningful changes in the general practices of academic journals in Korea, so long as the PIPA provisions that apply to academic journals do not differ from provisions in the GDPR.

With this in mind, the present article focuses on the implications of the GDPR and the PIPA for academic journals. To begin, a basic understanding of the concept of personal data and the laws protecting such personal data—the GDPR and the PIPA—are necessary.

How Can We Define "Personal Data"? Why Should We Care About Them?

"Personal data" refers to any information relating to a data subject—an identified or identifiable living person (not a legal entity). Different pieces of information that, when collected together, can lead to the identification of a particular person also constitute personal data [6-8]. For example, all the information that *Science Editing* requires for registration, such as a user's ORCID, email, name, affiliation and department, degree, address, and phone and fax numbers, falls in the category of personal data. Moreover, any information about registered users that was created after their registration (e.g., the results of a peer review, editorial decisions, turnaround time, and/or any comments on authors or reviews) also falls under this umbrella [5,9,10].

The EU laws provide that everyone has a fundamental right to the protection of his or her personal data [11,12]. Similarly, both Korea's Constitutional Court and Supreme Court have recognized individuals' rights to informational self-determination as a fundamental constitutional right. This is derived from the right to privacy (Korean Constitution Article 17) and the right to dignity and the pursuit of happiness (Korean Constitution Article 10) [13,14]. The GDPR and the PIPA embodied this fundamental right as the right to be informed, the right to consent, the right of access, the right to rectification and erasure, and so on under, which are basic laws protecting personal data in both the public and private sectors in the EU and Korea, respectively [GDPR Arts. 12–22, 34; PIPA Arts. 4, 35–37]. If a journal violates the GDPR or the PIPA, the journal might be subject to punishment or an administrative fine [GDPR Arts. 83, 84; PIPA Arts. 70–76]. Of course, an individual may also bring a civil claim against a journal that breached his or her personal data rights [GDPR Arts. 79, 82; PIPA Arts. 39, 39-2].

The GDPR Also Considers Academic Journals' Interests

There is also good news for academic journals. The right to the protection of personal data is not absolute [GDPR Art. 23]. GDPR Recital (4) states, "Personal data must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality." Indeed, the GDPR provides for many derogations or exemptions from its certain provisions based on "journalistic purposes and the purposes of academic, artistic or literary expression" or "archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes" [15,16]. The PIPA also provides for some provisions on derogations or exemptions [PIPA Arts. 35(4)(ii), 37(2)(ii), (iv), 58(1)].

What Should Academic Journals Then Do Or Not Do With Personal Data?

Collection of personal data

Journals should not collect more personal data than needed. Collect the data in a lawful manner and for specified, explicit, and legitimate purposes [GDPR Art. 5(1)(a) and (b); PIPA Arts. 3(1), (2), 16(1)]. Journals collect personal data for publication and communication regarding journal activities. Thus, in general, the scope of personal data that journals collect will likely not exceed the scope of information that *Science Editing* collects, as illustrated above. If sensitive personal data (e.g., race, political opinions, and religious or philosophical beliefs) are necessary for a journal, the journal must inform the data subject of its purpose and obtain informed and explicit consent from the data subject [GDPR Art. 9 (2); PIPA Art. 22(3)].

Journals may also collect personal data on potential authors or reviewers from publicly available information. This collection method is generally lawful because the data subject can be deemed to have consented to the collection or processing of his or her personal data within certain parameters [17]. A journal, however, should keep a record of the sources of the data, of which his or her journal has a legal duty to inform the data subject [18,19].

Disclosure of personal data protection policy

For a data subject to exercise his or her rights, the data subject must be aware of who collects his or her personal data, how the data is used, and, if the data is provided to a third party, which third parties receive the data. Therefore, a journal must establish and disclose such matters (i.e., a journal's personal data protection policy) to a data subject when collecting personal data, not only when the journal collects personal data from the data subject but also when obtaining personal data from other sources [PIPA Art. 30].

Sharing personal data with others

Journals should treat personal data as confidential information and share it only for the purpose of the journal activities of which a data subject has been informed. When sending newsletters regarding a journal's activities to multiple recipients, for example, using the "Bcc" field will conceal recipients' personal details from each other. If a journal provides offline subscriptions or sends hard copies to authors or reviewers, it can share recipient names and addresses with the printers. However, it must make sure that the printers do not use this information for any other purpose.

Considering that some reviewers or contributors are in foreign countries (especially countries outside the EU), some journals that adopt single-blind peer review or open-peer review policies might have concerns about the issue of transferring personal data to a third country, which is often mentioned in connection with the enforcement of the GDPR. The GDPR has restrictions about transferring personal data to a non-EU member state and allows it only when special conditions are satisfied [GDPR Art. 44]. Academic journals, however, need not be unduly concerned because the GDPR allows exemption or derogation for them [GDPR Arts. 49 (1) (b), 85(2)].

The rights to access, rectification, and erasure

In general, a journal, as a data controller, should be able to provide, rectify, or remove information upon a request from a contributor, a reviewer, or a subscriber [GDPR Arts. 15–17; PIPA Arts. 35–36]. For instance, if a reviewer wants to check his or her record on a journal, such as turnaround time, rating, or ranking, the journal is supposed to comply with that request. If the reviewer finds inaccurate data and requests rectification of that data, the journal must comply with that request as well.

In some cases, however, journals may have difficulty complying with certain requests from a data subject: if a contributor wants to access confidential comments on his or her article made exclusively for use by an editor; if a reviewer requests deletion of all the records on himself or herself; or if a rejected contributor requests deletion of all the data created regarding his or her contribution and its review. Although the laws are not discernable in all situations, the relevant laws consider not only the rights of a data subject but also the interests and rights of the other party—in this case, a journal [GDPR Arts. 17(3)(a), (d), 85(1), (2), 89(2); PIPA Art. 35(4)(ii)]. In other words, if a data subject's demand is deemed to undermine an academic journal's special function of publishing research and scholarship and the journal's needs that are pertinent to retaining a historical record of the process involved in reviewing and editing such research and scholarship, the journal can (at least partially) refuse such a demand from a data subject if it explains its reasons for doing so.

Conclusion

There is some criticism that the GDPR imposes a heavy burden in today's information-oriented society. However, it must be noted that the GDPR aims to balance the need to protect personal data with other important interests, including freedom of expression and information. In that regard, a journal that has treated personal data with respect need not be very concerned about the GDPR. For a comparison of the GDPR and the PIPA, see Appendix 1.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgments

This work was supported by the research program at Dongguk University.

References

1. Wall A. GDPR matchup: South Korea's Personal Information Protection Act [Internet]. Portsmouth, NH: International Association of Privacy Professionals [cited 2018 Dec 9]. Available from: https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act
2. Shon GR. Many differences between Korean, EU data protection laws. Korea Times. 2018 Jun 30 [cited 2018 Dec 9]. Available from: http://www.koreatimes.co.kr/www/opinion/2018/09/726_251463.html
3. Ministry of the Interior. Guidance on "General Data Protection Regulation" for Korean enterprises. Seoul: Ministry of the Interior; Korea Internet Security Agency; 2017.
4. Ahn CS. GDPR impact on Korea [Internet]. Panel discussion. 2018 Jun 25 [cited 2018 Dec 9]. Available from: https://

medium.com/@parallel38/gdpr-impact-on-korea-9eadbcecb54d
5. Lee CB. Commentaries on laws, guidelines, and public notices on personal data protection. Seoul: Ministry of Government Administration and Home Affairs; 2016.
6. General Data Protection Regulation Recitals (14), (26), (27), (30) and Article 4(1).
7. Personal Information Protection Act Article 2(1) and (3).
8. European Commission. What is personal data? [Internet]. Brussels: European Commission [cited 2018 Nov 26]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en#examples-of-personal-data
9. Court of Justice of the European Union. Case C-434/16 (December 20, 2017).
10. Purtova N. The law of everything: broad concept of personal data and future of EU data protection law. J Law Innov Technol 2018;10:40-81. https://doi.org/10.1080/17579961.2018.1452176
11. Charter of Fundamental Rights of the European Union. Article 8(1).
12. Treaty on the Functioning of the European Union. Article 16(1).
13. Supreme Court of Korea. 96da42789 (July 24, 1998).
14. Constitutional Court of Korea. 99hunma513, 2004hunma190 (consolidated) (May 26, 2005).
15. General Data Protection Regulation. Article 85(2).
16. General Data Protection Regulation. Articles 5(1)(b), (e), 9(2)(j), 14(5)(b), 17(3)(d), 21(6), 89.
17. Supreme Court of Korea. 2014da235080 (August 17, 2016).
18. General Data Protection Regulation. Article 14(2)(f).
19. Personal Information Protection Act. Article 20.

Appendix 1. Comparison of the GDPR and the PIPA

		GDPR	PIPA
Definition	Personal data & data subject	Art. 4(1)	Arts. 2(1),(3)
	Data controller/*Gaeinjeongbocheolija*	Art. 4(7)	Art. 2(5)
	Gaeinjeongbocheolichwigeubja	Art. 29	Art. 28(1)
	Data processing	Art. 4	Art. 2(2)
Basic principles		Art. 5	Art. 3
Rights of the data subject	Right to be Informed	Arts. 12, 13, 14, 19	Arts. 4(1), 15(2), 20
	Right to consent	Arts. 4(11), 7	Arts. 4 (2), 22
	Right of access	Art. 15	Arts. 4(3), 35
	Right to rectification and erasure	Arts. 16, 17	Arts. 4(4), Arts. 21, 36
Restrictions to rights of data subjects		Arts. 23, 85, 89; Arts. 14(5), 17(3), 18(2), 20(3), (4), 21 (6), 22 (2)	Arts. 35(4), 36(1), 37(2), 58(1)
Notification of a personal data breach		Arts. 33, 34	Art. 34
Compensation		Arts. 79, 82	Arts. 4(5), Arts. 39, 39-2
Fines/penalties		Arts. 83, 84	Arts. 70–76

GDPR, General Data Protection Regulation; PIPA, Personal Information Protection Act.