Open Net (Korea) | 402, 62-9 Seochodaero 50-gil, Seocho-Gu, Seoul, Republic of Korea (zip code) 06650 master@opennet.or.kr

Wojciech Wiewiorówski
European Data Protection Supervisor

March 25, 2021

Dear Mr. Wiewiorówski,

We, Open Net Association, Inc., an Observer to the Consultative Committee of Convention 108 and a United Nations Economic and Social Council (ECOSOC) Consultative Status Holder would like to submit information that we believe are relevant to the GDPR adequacy decision on South Korea as follows:

The South Korean legislature passed an amendment to each of the Personal Information Protection Act in February 2020 (Personal Information Protection Act, amended February 2, 2020, "K-PIPA", hereinafter)[1]. The most important purpose of the amendment was to adopt GDPR provisions that allow non-consensual use of personal data for public interest archiving, scientific research, or statistics ("ARS") purposes (GDPR Article 89(1)) and thereby promote data innovations. GDPR allows such non-consensual use only when "data minimization principles" are upheld such as through "pseudonymization" (GDPR Article 89(1)). Pseudonymization is the process of removing from personal data all information that may help identify the data subjects and replacing them with codes that are not readily available to others but later can be used to re-identify data subjects.

Requirement of publication of scientific research

GDPR allows "privately funded research" to be done under the ARS exception (GDPR Recital 159) and the K-PIPA amendment does the same. However, "privately funded research" allowed by GDPR still need to take into account the purpose of "European Research Area" set forth in Treaty Forming European Union, an idea that research is readily available within EU across national boundaries (GDPR Recital 159) and the K-PIPA amendment does not make reference to any such guiding principle. Reference to "European Research Area" implies that publication of the research to the public is required to benefit from the non-consensual ARS uses. We believe that such a requirement is consistent with an idea that non-consensual use is justified by

[1] available at https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=53044

countervailing public interest[2] and such public interest can be served by sharing the research with the greater society.

Therefore, the newly amended K-PIPA does not have any such reference or guiding principle, and therefore many privately funded research, for instance, for private marketing purposes without any "general public interest" whatsoever[3], can be conducted without the consent of data subjects.

Data subjects' access and other rights to pseudonymized data

Under GDPR, the authority of data controllers to use data for a new purpose without data subjects' consent is derived from the socially beneficial nature of the new purpose (i.e., science, statistics, public interest archiving). Such social benefit is deemed to justify the 'sacrifice' made by data subjects whence the data originated. Pseudonymization by itself does not have any socially beneficial aspect that will justify forfeiture of the data subjects' interest and yet became the linchpin for allowing non-consensual use in K-PIPA amendment. Pseudonymization is simply one of the measures achieving data minimization, a prerequisite for such non-consensual use (GDPR 89(1)). Likewise, under Korean PIPA, pseudonymized data could be used non-consensually only for ARS uses anyway (K-PIPA 28-2).

However, the consent power for use and transfer of data is not the only right that data subjects have. Data protection laws give data subjects other rights such as the right to inspect data about them held by data controllers, opt out of certain uses, and delete or correct data about them ("data subject's access and other rights"). Now, GDPR builds exemptions from these data subjects' rights into ARS non-consensual processing lest data innovation be frustrated when quality of data is deprecated by too extensive data subjects' exercises of access and other rights (GDPR 89(2)).

This is where Korea's PIPA widely departs from GDPR, wreaking havoc on the entire design of ARS exemptions. Under GDPR, it is ARS processing that triggers exemption from data subjects' access and other rights: in contrast, it is pseudonymization that triggers the same exemption (K-PIPA 28-7). The first problem is that any data controller can evade the duty to afford data subjects access, erasure, and objection simply by pseudonymization of the data even if it is not planning to use the resulting data for any socially beneficial purposes such as ARS purposes.

The government justifies this mishap as follows: '*ALL instances of reidentification of pseudonymised data are banned with criminal penalties without any exception (K-PIPA 28-5), and therefore, right of access,*

[2] See European Data Protection Supervisor, A Preliminary Opinion on Data Protection and Scientific Research, January 2020. "For the purposes of this Preliminary Opinion, therefore, the special data protection regime for scientific research is understood to apply where each of the three criteria are met: 1) personal data are processed; 2) relevant sectoral standards of methodology and ethics apply, including the notion of informed consent, accountability and oversight; 3) the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests."
See the Opinion of AG Mancini in Case 234/83 *Gesamthochschule Duisburg v Hauptzollamt München-Mitte* [1985] on interpretation of 'scientific activities' in the context of the legislation relating to custom duties (first indent of Article 3(2) of Regulation No 1798/75): 'scientific activities must be interpreted as including activities carried on by a public or private establishment engaged in education or research for the purpose of further the acquisition, development, exposition or dissemination of scientific knowledge (...)'.

[3] "Commercial scientific research may therefore be covered, but you need to demonstrate that it uses rigorous scientific methods and furthers a general public interest. However, commercial market research is unlikely to be covered, unless you meet this requirement."
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/

erasure/correction, and objection cannot be afforded anyway.' However, this does not answer the fundamental question: why should data subjects' access, erasure, and objection rights be abrogated simply because data are pseudonymized?

Pseudonymization is a process explicitly encouraged by GDPR for security and privacy purposes (GDPR 32, 40). German data protection law also requires pseudonymization as part of security measures (BDSG Article 64) and privacy by design (Article 71) and also requires that personal data be pseudonymized or anonymized as soon as possible and as much as possible to the extent compatible with the purpose of collection (BDSG Article 71). Storing all unique identifiers of data files such as names, credit card numbers, social security numbers, etc., in the form of encrypted codes is a routine practice. Korean law even requires residence registration numbers to be stored only in encrypted form (Korea's Personal Data Security Measures Standard (a regulation promulgated under and interpreting Korean Personal Information Protection Act) Article 7). It is therefore not equitable for data subjects to couple such routinely used and sometimes legally compelled process with deprivation of data subjects' access and other rights.

What is more, now that pseudonymization has become a dangerous process for data subjects, the government has come up with cumbersome prerequisites for pseudonymization, which makes it difficult for data controllers to engage in security measures involving pseudonymization and encryption. It is true that pseudonymization and encryption are still 'data processing' and therefore doing so non-consensually still requires some legal basis (GDPR 6) but given that pseudonymization is explicitly encouraged by GDPR for privacy and security, in "all conceivable cases", pseudonymization will be considered compatible with the original purpose of collection. So, it has the result of disincentivizing good-willed data controllers from taking pseudonymization for privacy-enhancing and security-enhancing purposes. Now, data subjects suffer either way because data controllers cannot take privacy/security-enhancing measures due to the cumbersome prerequisite to pseudonymization and also because, if they somehow succeed in pseudonymizing the data, their access, erasure/deletion, and opt-out rights are abrogated in disregard to whether pseudonymization may bring any social benefit.

Civil society organizations are so concerned with deprivation that they have filed a constitutional challenge against Articles 28-5, 28-7 of K-PIPA.[4]

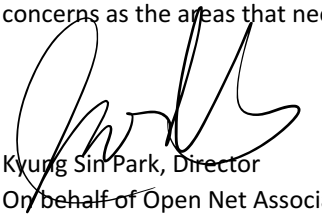
In defending the K-PIPA amendment, some may cite data protection law of Japan, the country that has passed the adequacy decision previously, which has enacted the concept of 'anonymously processed data' and also criminalizes re-identification for all purposes by anyone and treats it as non-personal data (Act for Protection of Personal Information, Article 36(5), Article 38)[5], thereby depriving all data subjects all the rights they would have had if the data were personal. This is different from pseudonymized data under GDPR and Korean PIPA, which is built on the premise that it can be re-identified and therefore it is still considered personal data subject to data subjects' access and other rights. It is for this reason that Japan made an amendment in 2020 that created a new concept of 'pseudonymously processed data' that corresponds to pseudonymized data under GDPR and K-PIPA.[6]

[4] https://www.hankyung.com/society/article/202011025040i (Korean only)
[5] available at http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=04&re=2&new=1
[6] https://www.natlawreview.com/article/new-amendments-passed-to-japan-s-data-privacy-law

Others cite Article 11 of GDPR to justify deprivation of data subjects' access and other rights for pseudonymised data. However, it is well established that GDPR Article 11 should not be used as a pretext for evading data subjects' exercise of access and other rights on pseudonymised data.[7]

Conclusion and Recommendation

In conclusion, we believe that, for a data protection law to function properly, the non-consensual use of people's data must be allowed only when such use creates social benefits, as GDPR does. To that end, firstly, the non-consensual scientific research exception should require publication of the research. Secondly, data subjects' access and other rights should be abrogated only in exchange for socially beneficial purposes such as ARS purposes (Article 28-7), not just for pseudonymization. Thirdly, Article 28-5 be amended so that pseudonymized data can be re-identified for the purpose of affording data subjects the access and other rights. Hope that the adequacy review takes into account these points. Even if this submission does not affect the ultimate result of the adequacy review for some reason, we hope that the decision at least mention these concerns as the areas that need be addressed in the future.



Kyung Sin Park, Director
On behalf of Open Net Association, Inc.
kyungsinpark@korea.ac.kr

7 https://iapp.org/news/a/article-11-gdpr-processing-data-that-does-not-require-identification-and-how-it-should-not-be-interpreted/