# Improving Data Privacy for Japan －APPI and GDPR Case Study

## 日本におけるデータプライバシーの改善 －APPI と GDPR のケーススタディ

ヘマンギ ゴークレ※
Hemangi Gokhale※

**Abstract**

Steady digitization of societies and growth in data driven industries has made protecting data privacy of paramount importance. The Japanese government and EU Commission have been on the forefront of designing data privacy regulations for the 21st century. Japan's Act on the Protection of Personal Information (APPI) (Act No. 57) and EU's General Data Protection Regulation (GDPR) are landmark regulations that provide insights into regulatory frameworks that attempt to balance tech innovation with data privacy rights. This paper briefly reviews the two regulations and proposes suggestions to improve APPI effectiveness. Specifically, the paper considers applicability of GDPR's data breach penalty mechanism and considers other measures to improve data industries' compliance with APPI data privacy standards.

**Keywords**:Data Privacy, Japan, APPI, GDPR.

## 1. Introduction:

The 21st century has seen an unprecedented growth in data driven industries. Governments have also actively embraced digitization of economies[1]. 'Fourth industrial revolution' products such as big data, internet of things (IoT), cloud computing, 3D printing, and artificial intelligence are heavily data driven[2]. Big data analytics have become key to enhancing market and industry competitiveness. Data, including personal data, has thus become a valuable economic commodity. In Japan and the European Union (EU), personal data is perceived as an individual's constitutional right. In Japan, Article 13 of its constitution implicitly implies an individual's right to data privacy (Ishii and Komukai, 2016; Wang, 2020)[3]. Similarly, the EU commission recognizes data privacy

*Associate Professor, Department of Global Business Administration, Japan University of Economics.
***This paper was supported by 2022 research grant from Japan University of Economics.

[1] 2017 G20 meeting: Roadmap to digitilization (Policies for a digital future). Source: http://www.g20.utoronto.ca/2017/170407-digitalization-annex1.html

[2] Schwab, K. (January 14, 2016). "The Fourth Industrial Revolution: what it means, how to respond." World Economic Forum. Source: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[3] The constitution of Japan. Source: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html

as a human right[4]. Recently, data breaches and data security violations have increased in tandem[5, 6, 7]. Thus, addressing personal data protection and enhancing market competitiveness of data driven industries has become a high priority issue for the two economies.

In light of data-driven socio-economic changes, Japanese government and the EU commission have proactively designed regulatory frameworks that attempt to balance incentives for industry innovation with domestic data security requirements and data rights. In 2017 and 2022, Japan amended the 2004 Act on Protection of Personal Information (APPI) to be in compliance with the Japanese constitution and to meet industry expectations for enhanced data access[8]. Similarly, in 2018, the EU commission implemented a comprehensive regulatory data governance framework, the General Data Protection Regulation (GDPR)[9], which provided EU citizens with greater control over their data and offered guidance to data-based industries on data handling requirements. In January 2019 at the Osaka G20 summit, former Japanese Prime Minister Shinzo Abe proposed that world governments work together on a global data governance framework that would allow global economies to facilitate cross-country information flow while addressing data security concerns[10]. A concept of "Data Free-Flow with Trust (DFFT)" was put forth accordingly at the summit. While DFFT did not make headway, in 2019 Japan and EU signed a Data Adequacy Agreement that allowed for free flow of personal data between the two regions[11]. Japan and EU are important trade partners and attractive destination markets for global economies. Thus, Japan's APPI and EU's GDPR regulations have strong implications for businesses and organizations that handle Japanese and EU citizens' data, or conduct business in the Japanese or EU markets.

APPI and GDPR regulations are progressive in being on the forefront of regulatory frameworks for the digital era; however, the two regulations are not without limitations. For instance, GDPR has strong penalty enforcement mechanism that incentivizes compliance amongst data industry businesses. However, as data security tech solutions have not kept pace with broader data applications[12], data security compliance for businesses tends to come at a cost to data utility[13]. On the other hand, while APPI applies lower penalty

[4] EU Data Privacy. Source: https://edps.europa.eu/data-protection/data-protection_en
[5] Data breaches in the US. Source: https://privacyrights.org/data-breaches
[6] Data breach penalties in EU. Source: https://www.enforcementtracker.com/
[7] Japan Personal Information Protection Commission (PPC) 2021 annual report (in Japanese). Source: https://www.ppc.go.jp/files/pdf/040610_annual_report_gaiyou.pdf
[8] Japan Personal Information Protection Commission (PPC). Source: https://www.ppc.go.jp/en/legal/
[9] EU General Data Protection Regulation (GDPR) legal text. Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[10] Ministry of Foreign Affairs of Japan (MoFA). (January 23, 2019). Speech by Prime Minister Abe at the World Economic Forum Annual Meeting. Toward a New Era of "Hope-Driven Economy." Accessed May 20, 2022. Source: https://www.mofa.go.jp/ecm/ec/page4e_000973.html
[11] EU Commission Announcement on Japan-EU Data Adequacy Agreement. Source: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421
[12] https://www.nature.com/articles/s41467-019-10933-3
[13] Changing data treatment 'can affect data analysis, which may affect (firm's) bottom-line'. Knowledge at Wharton. Source: https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/

threshold to incentivize innovation in data industries, lower penalties have not been able to reign in lax data security standards applied by data industries. This paper briefly reviews Japan's APPI and EU's GDPR regulations, and proposes suggestions to improve APPI effectiveness. Specifically, the paper considers applicability of GDPR's data breach penalty mechanism and considers other measures to improve data industries' compliance with APPI data privacy standards.

## 2. Japan's Act on Protection of Personal Information (APPI):

The Japanese constitution and Tort case laws implicitly hint at data privacy as a constitutional right (Ishii and Komukai, 2016; Wang, 2020). Japan's 2004 Act on Protection of Personal Information (APPI) aims to create a regulatory framework that allows for emerging industries to thrive while protecting data privacy rights of Japanese citizens[14]. The Act gets amended periodically to address changes in industries' data handling and data flow norms, with the latest amendment to the regulation being in 2020[15].

APPI is comprehensive in its guidelines. It defines 'personal information' as any information relating to a living person that can be used to identify an individual directly or indirectly, 'stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record'[16]. It also provides guidance on retained personal data and defines 'personal information database' as an assembly wherein information is 'systematically arranged' and specific information can be easily retrieved (Ishiara, 2021). APPI includes requirements and guidance for 'personal information handling business operators' in regards to data subjects' consent, data accuracy and treatment protocols (including guidance on anonymous and pseudonymous data treatment[17]), data security guidance, advice on physical safeguards to minimize or limit personal data exposure within the firm, and data handling requirements for instances when personal data is collected by business operators 'for business purposes.' However, APPI uses broad language in the regulation and does not define business operator activities that may be in scope for compliance.

APPI also includes details on data subjects' rights. Per APPI, data subjects have a right to personal data disclosure, data correction, right to discontinue personal data utilization, right to data erasure and right to legal action. However, it does not specify any steps a data subject may pursue to exercise data privacy rights. APPI requires business operators to notify data subjects on matters of data collection, data sharing, data maintenance

[14] Japan 2004 APPI Act, Article 1. Source: https://www.ppc.go.jp/files/pdf/APPI_english.pdf
[15] Japan PPC: APPI amendments and laws. Source: https://www.ppc.go.jp/en/legal/
[16] Personal information includes personal details on name, date of birth, address, or any description that can be identified with the individual, 'special care' details i.e. information in regards to an individual's medical history, marital status, race, religious belief and such that may cause discrimination, and identification codes such as characters, letters, numbers, or symbols assigned at the time of selling goods and services to the individual and that could be used to identify an individual. Source: https://www.ppc.go.jp/files/pdf/APPI_english.pdf
[17] Japan PPC. Source: https://www.ppc.go.jp/files/pdf/APPI_english.pdf

and data breaches. It requires business operators to make available details on data elements collected, purpose and methods of data collection, data sharing arrangements, and data retention periods. Additionally, APPI has mandatory requirements for business operators to notify data subjects and government authorities about incidents of data breaches and data security violations. APPI also requires business operators to notify Japanese data subjects when personal data gets shared with other business partners. APPI thus, to a certain extent, addresses extraterritorial data flows and third-party data sharing arrangements that are prevalent in data driven industries. However, APPI does not extend Japanese data subjects' data security rights when data leaves the Japanese jurisdiction. It simply includes guidance on data subject notification and data subject's right to discontinue data utilization in such instances.

Finally, to ensure compliance with APPI data security standards, the regulation has penalty enforcement measures for data breaches, data security violations and non-compliance. For instance, depending on the nature of data security violation, extent of participation, and damage caused[18], APPI allows a criminal penalty fine of JPY 300,000 (about EUR 2,113) to JPY 1 million (approximately EUR 7,047) or imprisonment with labor for six months to two years. Additionally, in instances of intentional or non-intentional false reporting to authorities, fine of up to ¥500,000 (approximately EUR 3,523) can be levied. In non-criminal cases, APPI allows for fines up to JPY 100,000 (about EUR 704) on individuals or business operators on non-compliance charges[19, 20].

## 3. EU's General Data Protection Regulation (GDPR):

In EU, data privacy is considered a human right. Per EU Commission, the notion of data privacy is embedded in EU citizens' right to a private life, anonymity, control over one's information and right to be let alone[21]. Thus, in light of the unprecedented growth in data driven industries, in 2018, EU Commission implemented the General Data Protection Regulation (GDPR)[22].

Similar to Japan's APPI, EU's GDPR provides data subjects (EU citizens) greater control over the collection, distribution, utilization and retention of their personal data. GDPR defines personal data very broadly. Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject') such that an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[23]"

[18] Tort law application (Ishii and Komukai, 2016; Wang, 2020).
[19] JPY-EUR exchange rate as of September 2022.
[20] PPC APPI penalty guidelines. Source: https://www.ppc.go.jp/files/pdf/APPI_english.pdf
[21] EU Commission, EDPS. Source: https://edps.europa.eu/data-protection/data-protection_en
[22] GDPR legal text. Source: https://gdpr-info.eu/
[23] GDPR personal data definition. Source: https://gdpr.eu/eu-gdpr-personal-data/

GDPR has several data identification, monitoring and reporting requirements for 'data controllers[24] and data processors[25]'. Data controllers are required to have a detailed and updated list of all personal data processing activities including details of data controller or individuals handling personal data, data elements collected, purpose of data collection and processing, details on recipients of personal data, third party data sharing arrangements and cross-country data transfers, (if possible) expected time limits for data erasure, and (if possible) details about firm's general data security measures. GDPR also requires businesses to provide a legal justification for collection of user data, have a mechanism in place to collect and report consents obtained on data collection from EU data subjects, and have a privacy policy in place to communicate the purpose of firm's data collection and processing activities in a manner that is concise, transparent, easily understood and is in plain language for data subjects to comprehend.

GDPR also has several data security requirements for data controllers and data processors. For instance, GDPR advices data controllers to apply data protection 'by design and by default' so that measures such as data encryption, anonymization, pseudonymization are applied wherever possible, and data collected is minimized and limited to the legal justification for original data collection purposes[26]. Additionally, data controllers are allowed to transfer personal data and work with only those data processors that provide 'sufficient guarantees' in regards to meeting GDPR compliance measures[27]. GDPR also extends compliance requirements to data processors such that originally partnered data processors are not allowed to enter into new third party data processor arrangements without the prior knowledge and consent of the originally contracted data controller. All data processors working with or having access to EU citizens' data are also subject to GDPR compliance requirements. The regulation additionally requires data controllers to have high data security protocols and standards, and recommends periodic 'data protection impact assessment' to reduce risks from data leakage and data breaches. While GDPR includes several details on requirements and guidance for data controllers and processors, similar to APPI, it does not specify tech solutions or methods that businesses may pursue to meet regulatory compliance.

GDPR, similar to APPI, also provides detailed guidance on rights of EU data subjects. The regulation gives EU data subjects right to details on personal data collected, data retention periods and data collection purpose, right to data correction and erasure, right to discontinue utilization of personal data, and right to legal action[28]. However, similar to APPI, GDPR does not specify steps that an individual may take to exercise ones right and the methodology is left to individual discretion.

---

[24] GDPR compliance checklist for data controllers. Source: https://gdpr.eu/checklist/
[25] GDPR compliance requirements for data processors. Source: https://gdpr.eu/article-28-processor/
[26] Source: https://gdpr.eu/article-25-data-protection-by-design/
[27] GDPR Data processor requirements. Source: https://gdpr.eu/article-28-processor/
[28] Source: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/redress/can-i-claim-compensation_en

Finally, given the EU understanding of data privacy as a human right, GDPR imposes strong penalties for data security violations, data breaches and non-compliance. For instance, in cases of data security violations, EU courts may levy fine up to EUR 20 million, or in the case of an undertaking, up to 4 % of a company's total global turnover of the preceding fiscal year, whichever is higher. For relatively less severe violations as well, GDPR allows for fines up to 10 million euros, or, in the case of an undertaking, up to 2% of a company's entire global turnover of the preceding fiscal year, whichever is higher. However, penalty fees may not necessarily be high. Depending on the details of an individual case, nature of GDPR violation and parties involved, individual EU states may levy relatively lower penalty fees as well[29, 30].

## 4. APPI compliance enforcement mechanism and data breaches:

Japan's APPI law provides a regulatory framework that incentivizes business growth and innovation in data driven industries, while safeguarding data security. Japan's APPI is also relatively business friendly. In fact, unlike GDPR, Japan's APPI recognizes data as an economic commodity and protects a relatively narrow category of personal information to allow for business growth in the private sector (Wang, 2020).[31] While Japan's APPI has high data privacy standards, the regulation is not overly taxing to the private sector. For instance, APPI does not specifically define business activities in scope for compliance, does not make separate compliance requirements for data processors and data controllers, broadly requires business operators to apply appropriate data security protocols, has relatively less data identification, tracking, monitoring and reporting requirements (as compared to GDPR), is not overreaching in its compliance measures, and has relatively lower penalty fees. The Japanese APPI enforcement approach has worked relatively well in the past. However, in the last decade, data breaches and data security violations related to Japanese personal data have increased (as they have globally). Thus, there is a need for further amendments to Japan's APPI enforcement mechanism.

APPI penalty and compliance structure while generally effective, is not immune to limitations. Currently, APPI applies criminal sanctions only when all other avenues for recourse have been exhausted. While APPI allows for data subjects to take legal action against business operators, it does not clearly define 'injury' or 'harm' (Wang, 2020). Thus, even after data subjects engage in legal action with a business operator, consumers may not be appropriately compensated. Additionally, Japan's APPI enforcement mechanism is designed with the understanding of Japanese 'cultural values and social norms' wherein 'privacy' is actually an imported concept, and reputation risk and social pressure play a stronger role in motivating Japanese business operators to meet data security obligations and APPI compliance (Orito and Murata, 2005; Wang, 2020).

---

[29] GDPR Penalty and Fines. Source: https://gdpr-info.eu/issues/fines-penalties/

[30] GDPR penalty enforcement tracker. Source: https://www.enforcementtracker.com/

[31] For instance, computer cookie IDs and IP addresses are not considered to be personal information if it cannot be readily collated with other details to identify a data subject. Source: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

While business data operators and institutions in Japan have shown strong commitment towards APPI compliance, data breaches and data security compromises continue to be frequent. For instance, in 2014, a part-time contractor of a Japanese educational company (Benesse corporation) illegally stole and sold personal details of the company's 7.6 million customers. The customer data was sold to three data brokers before the matter became known to Japanese authorities (Ishii and Komukai, 2016). Per Tokyo Shoko Research Ltd. survey, in 2019, data leaks from 32 publicly traded companies in Japan resulted in personal data security violation of 8.9 million workers and customers[32]. Similarly, a survey conducted in 2021 indicated that the number of personal data leaks from firms listed on the Japanese stock exchanges and their subsidiaries rose by 30% to 137 cases. Per survey, half of the data security violations came due to unauthorized access to personal data and malware[33]. Most recently in 2022, Amagasaki city representative in Western Japan lost a USB flash drive that contained personal data and bank details of all of its roughly 460,000 residents[34]. Thus, APPI enforcement mechanism needs to be strengthened to incentivize businesses to invest more actively in strong data security measures.

Additionally, there may be a need to consider stronger penalty clause to meet the international threshold standards of fines and compensation structures. In certain cases where Japanese data subjects have taken legal action for data security violations, penalty fees imposed and injury compensation does not seem to be adequate. For example, in the Benesse case where 29 million pieces of Japanese customer data was sold, victims were given JPY500 coupons for injury compensation (Ishii and Komukai, 2016). The Benesse case prompted amendments in the APPI enforcement mechanism. However, current penalty structure is still not effective in making data security compliance to be an urgent business priority. For instance, in 2020 when Google failed to adequately notify data subjects that their personal data was shared with advertisers, the French data protection authority levied a fine of EUR 50 million on Google for violating GDPR compliance. On the other hand, Japanese authorities only warned Google to be careful in regards to APPI compliance (Wang, 2020). Similarly in 2016 when Facebook Cambridge Analytica scandal came to light, Japanese authorities learnt that the data breach had potentially affected 100,000 Japanese data subjects. While U.S. Federal Trade Commission (FTC) levied a fine of USD 5 billion on Facebook for data security violations, Japanese authorities were only able to advice Facebook to improve its data security measures (Wang, 2020).

## 5. Potential solutions for APPI enforcement mechanism and GDPR approach:

Japanese APPI enforcement mechanism requires amendments to motivate businesses to handle and process

[32] Japan Times (January 24, 2020). Personal info of 8.9 million in Japan compromised by viruses and unauthorized access in 2019. Source: https://www.japantimes.co.jp/news/2020/01/24/national/virus-access-compromised-info-millions-japan/

[33] Japan Times (February 23, 2022).Personal info leaks from listed Japan firms hit record high in 2021. Source: https://www.japantimes.co.jp/news/2022/02/23/business/japan-firm-infoleak/

[34] Nikkei Asia (June 23, 2022). Japan city loses memory drive with data of all 460,000 residents. Nikkei Asia. Source: https://asia.nikkei.com/Spotlight/Society/Japan-city-loses-memory-drive-with-data-of-all-460-000-residents

data in a more secure manner. One way to reach this objective is to apply a stronger penalty structure similar to GDPR. A percentage penalty fee format based on business revenue can be levied such that penalty fees are applied proportionate to business size and data leak-based business revenue generated. Another way is for APPI to extend regulation compliance requirements to any third party or cross-country data brokers and data handlers such that currently out-of-scope businesses that benefit from data leaks can be held liable for profiteering from compromised personal data. APPI can also require data security measures at design level[35]. Finally, APPI compliance expectations can be further detailed such that there is uniform understanding of APPI compliance requirements amongst Japanese and non-Japanese firms.

## References:

Ishiara, T. (October, 2021). Japan. *Privacy, Data Protection and Cybersecurity Law Review. Eighth Edition* (pp. 241-263).

Ishii, K. and Komukai, T. (September 7-9, 2016). A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K. In Kreps, D., Fletcher, G., Griffiths, M. (Eds). *Technology and Intimacy: Choice or Coercion. HCC2016. IFIP Advances in Information and Communication Technology, vol. 474* (pp. 86-105). Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-44805-3_8

Orito, Y. and Murata, K. (September 2005). Privacy Protection in Japan: Cultural Influence on the Universal Value. ETHICOMP 2005 conference. Source: https://www.isc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf

Wang, F.Y. (2020). Cooperative data privacy: The Japanese model of data privacy and the EU-Japan GDPR Adequacy Agreement. Harvard Journal of Law and Technology. Vol. 33, no. 2, pp. 661-691.

[35] For instance, data anonymization and data pseudonymization at the local device data collection level.