Newsletter

Atsumi & Sakai

NEW DATA PROTECTION REGIMES IN THE EU AND JAPAN:

Similarities and Differences

ATSUMI & SAKAI
TOKYO | LONDON | FRANKFURT
www.aplaw.jp/en

September 2018

NEW DATA PROTECTION REGIMES IN THE EU AND JAPAN:
Similarities and Differences

The last two years have seen substantial revisions to the data protection regimes in Japan and the EU with the introduction of the Act on the Protection of Personal Information ("**APPI**") in Japan in 2017[1] and the General Data Protection Regulation ("**GDPR**") in the EU in 2018. In this newsletter, we highlight the key similarities of, and differences between the GDPR and the APPI.

1. Extraterritorial Application

Both the GDPR and the APPI have limited extraterritorial application.

GDPR	APPI
Can be applied to persons or entities which are not located inside the EU if their business provides goods or services to a person within the EU, or they monitor the data subject's behaviour within the EU.[2]	Can be applied to persons or entities which are located outside of Japan which have acquired personal information of a person resident in Japan as a data subject in relation to supplying goods or services to that person and handle that personal information in a foreign country.[3]

2. General Scope of Protected Data

Whilst there is some overlap between the general scope of the protection under the APPI and that under the GDPR, the general scope of the APPI is somewhat narrower than that of the GDPR as the APPI relates to identification of an individual, not information of an individual as under GDPR.

GDPR	APPI
Applies to "**personal data**" being "any information relating to an identified or identifiable natural person".[4] Examples include: ➢ name	Applies to information which allows the identification of a specific living individual in Japan (including information which can be easily combined with other information to enable the

[1] Please see our Newsletter, "Protecting Personal Information in the Age of Big Data – Japan's New Regime" ("APPI Newsletter") (*http://www.aplaw.jp/en/publications/20171221/index.html*) for a summary of the APPI.
[2] GDPR, Art. 3.
[3] APPI, Art. 75; see APPI Newsletter section 7.
[4] GDPR, Art 4(1).

➢ an identification number ➢ location data ➢ an online identifier (IP address) ➢ factors specific to physical, physiological, economic, cultural or social identity.	identification of such an individual) ("**personal information**"[5]).[6] Examples include: ➢ name ➢ date of birth ➢ DNA, face, iris ➢ fingerprints ➢ passport number ➢ Individual Social Security Number[7]

3. Exclusions for Holders of Small Amounts of Personal Information

GDPR	APPI
The GDPR regime applies to the processing of personal data wholly or partly by automated means and to processing other than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system. There are no exclusions for holders of small amounts of personal data.	The APPI regime applies to all holders of personal information who use it in connection with their business, regardless of the number of data subjects whose personal information is held.[8]

4. Data Given Additional Protection

Both the GDPR and the APPI include special protections for sensitive information, though the scope of the protections under the APPI is more limited than that under the GDPR.

GDPR	APPI
The processing of "**special categories of personal data**" is only permitted within a narrow	The consent of the data subject is required for the collection of "**special-care-required personal**

[5] The APPI also uses the term "Personal Data" though the terms "personal information" and "personal data" have different meanings and usages. When personal information is organized in a database and made searchable, it is called a "personal information database, etc." and the information that makes up the "personal information database, etc." is defined as "personal data".
[6] APPI, Art. 2(1). See APPI Newsletter section 2.
[7] Commonly known as "My Number"; these are also subject to a specific separate data protection regime.
[8] Prior to the introduction of the APPI, entities holding personal information on not more than 5,000 data subjects were usually exempt from Japan's data protection regime.

scope, such as pursuant to the data subject's explicit consent.[9] Special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning sex life or sexual orientation.	**information**", and its transfer to third parties is subject to restrictions, such as not allowing the use of an opt-out for consent.[10,11] Special-care-required personal information includes a data subject's race, faith, social status, medical history, criminal record, or other information requiring special consideration in its handling so that the data subject does not experience unfair discrimination, prejudice, or other harm.

5. Anonymous, etc. Information

Both the GDPR and the APPI address data subjects' concerns over the use of big data, though through different concepts and processes.

GDPR	APPI
The GDPR does not apply to "**anonymous information**", i.e. information which does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable[12], even if it is possible to process the information so that it would constitute personal data.	The APPI has a concept of "**anonymously processed information**", i.e. information regarding an individual which has been modified so that it cannot be used to identify the individual[13]; anonymously processed information retains that status even if it is possible to reprocess the information to personal information provided the means to reprocess it is securely and separately stored from the anonymously processed information.[14]

[9] GDPR, Art. 9.
[10] APPI, Art. 2(3), Art. 17(2), Art. 23 (2). See APPI Newsletter section 3.
[11] Under the APPI, information relating to trade union membership, sex life, and sexual orientation is not "special-care-required personal information." However, as discussed at footnote 48 below, it is anticipated that by the fall of 2018 the European Commission will certify Japan as a country with an adequate level of personal data protection ("**adequacy certification**"), and it is anticipated that along with such certification, guidelines will be put in place in Japan so that such information, when received from the EU area, will be treated in the same manner as "special-care-required personal information."
[12] GDPR, Recital 26.
[13] APPI, Art. 2 (9).
[14] It is anticipated that when the EU issues an adequacy certification in respect of Japan there will also be guidelines put in place in Japan that, for personal information which is received from within the EU, information will be deemed "anonymously processed information" only when the data controller deletes all information relating to any method of processing by which the original personal

	Anonymously processed information is not excluded from the application of the APPI but the obligations applicable to its handling are limited[15], e.g. it can be transferred without the data subject's consent provided certain notifications are provided.[16]

6. Obligations of Data Controllers[17] & Rights of Data Subjects

The table below gives a comparison of the main obligations of a data controller under the GDPR and a data controller under the APPI, and the main rights of a data subject against each.

GDPR	APPI
Lawfulness, Fairness and Transparency	
Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.[18]	A data controller must not acquire personal information by deceit or other improper means.[19]
Purpose Limitation	
Personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[20]	A data controller must specify the purpose of use of personal information and must only use the information within the scope of such purpose.[21]
Limitation of scope of content	
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.[22]	No relevant provision in the APPI.

information can be restored, and the re-identification of previously anonymized individuals is made impossible.

[15] APPI, Art. 36, et seq.

[16] See APPI Newsletter section 9.

[17] The APPI uses the term "personal information handling business operator," which means an individual or an entity which uses a database (electronic or otherwise) of personal information in its business. For simplicity, in this newsletter we assume that all data controllers are personal information handling business operators.

[18] GDPR, Art. 5(1)(a).

[19] APPI, Art. 17.

[20] GDPR, Art. 5(1)(b).

[21] APPI, Art. 15 and 16.

[22] GDPR, Art. 5(1)(c).

Accuracy	
Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.[23]	A data controller must strive to keep personal information accurate and up to date.[24]
Storage Limitation	
Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was processed.[25]	A data controller must strive to delete personal information without delay when the use of such information is no longer required.[26]
Provision of Information	
The data controller must provide the data subject with certain information such as the contact details of the controller, the purposes of the processing its personal data and the legal basis for the processing.[27]	A data controller must promptly inform the data subject of the purpose of use of its personal information, or publicly announce such purpose.[28] A data controller must state its name, the purpose for using all personal information, the procedures for requesting disclosure of personal information, and certain other matters, in such a way that it may be ascertained by the data subject[29].
Right of Access	
The data subject shall have the right to obtain from the data controller confirmation as to whether or not their personal data is being processed, and, where that is the case, access to the personal data and other information.[30]	The data subject may demand that the data controller disclose to the data subject personal information which it holds that can identify the data subject.[31]

[23] GDPR, Art. 5(1)(d).
[24] APPI, Art. 19.
[25] GDPR, Art. 5(1)(e).
[26] APPI, Art. 19.
[27] GDPR, Art. 13 and 14.
[28] APPI, Art. 18.
[29] APPI, Art. 27.
[30] GDPR, Art. 15.

Right to Rectification	
The data subject can require the data controller to rectify inaccurate personal data without delay. Considering the purposes of the data processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.[32]	A data subject may require the data controller to correct inaccurate personal information of the data subject.[33]
Right to Deletion / Right to be Forgotten	
A data controller must delete a data subject's personal data on the request of the data subject and without undue delay. A data controller must also erase personal data without undue delay in certain other cases, such as when the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.[34]	The data subject may require the data controller to delete personal information if it is not accurate, or if it is being used in a manner that exceeds the scope necessary to achieve the specified purpose of use or if it was acquired by deceit or other improper means.[35]
Right to Restrict Processing	
The data subject can require the data controller to restrict the processing of its personal data in certain cases.[36]	If personal information is being used in a manner that exceeds the scope necessary to achieve the specified purpose of use or if it was acquired by deceit or any other improper method, the data subject may demand that the data controller cease use of such personal information.[37]
Data Portability	
The data subject shall have the right to be given any personal data they provided to a data controller in a structured, commonly used and machine-readable format, and to transmit that data to another data controller without hindrance from	No relevant provision in the APPI.

[31] APPI, Art. 28.
[32] GDPR, Art. 16.
[33] APPI, Art. 29.
[34] GDPR, Art. 17.
[35] APPI, Art. 29 and 30.
[36] GDPR, Art. 18.
[37] APPI, Art. 30.

the data controller to which the personal data was originally provided.[38]	
Right to Object	
The data subject shall have the right to object, at any time to the processing of their personal data in certain cases.[39]	No relevant provision in the APPI.
Automated Individual Decision-making	
The data subject shall have the right not to be subject to a decision based solely on automated processing of their personal data, including profiling, which has a legal effect on them or similarly significantly affects them.[40]	No relevant provision in the APPI.
Processor	
Where processing is to be carried out on behalf of a data controller, the data controller shall only use data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.[41]	A data controller entrusting the handling of personal data, in whole or in part, to another person shall exercise necessary and appropriate supervision over the person entrusted to ensure the secure management of the personal information.[42]
Security of Processing	
Having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as to the risk to the rights and freedoms of natural persons, the data controller and the data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.[43]	In order to prevent the leakage, loss, or damage of the personal information that it handles, a data controller shall take necessary and appropriate measures for the secure management of personal information.[44] A data controller shall, in having its employees handle personal information, exercise

[38] GDPR, Art. 20.
[39] GDPR, Art. 21.
[40] GDPR, Art. 22.
[41] GDPR, Art. 28.
[42] APPI, Art. 22. Whilst the APPI does not provide a concept equivalent to "processor" under the GDPR, a party entrusted with data processing by a data controller and which the data controller is obligated to supervise would be included in the concept of "processor".
[43] GDPR, Art. 32.
[44] APPI, Art. 20.

	necessary and appropriate supervision over the employees to ensure the secure management of the personal information.[45]
Data Protection Officer	
The data controller and the data processor must designate a data protection officer in certain cases.[46]	No relevant provision in the APPI, though the need could be implied through the application of other general obligations on the protection of personal information.[47]

7. Transfer of Personal Information/Data Outside the Jurisdiction

GDPR	APPI
The transfer of personal data outside of the European Economic Area is lawful in certain cases, such as when the country to which the personal data is transferred is recognized as a country with an adequate level of personal data protection[48], or when appropriate safeguards are in place, or when the data subject consents to such a transfer.[49]	If it wishes to provide personal information to a "third party in a foreign country"[50], a data controller must first obtain the consent of the data subject, directly or by an opt-out[51]; the consent must make it clear that the transfer is to be to a third party in a foreign country, and the country identified, or identifiable by the data subject. If the consent is not obtained, or is given through an opt-out, the transferee or the country it is in must meet certain data protection standards[52,53]; if it doesn't, contractual protections will be required.

[45] APPI, Art. 21.
[46] GDPR, Art. 37.
[47] For example, the guidelines specifying the content of specific examples of security control measures as provided in Article 20 of the APPI; see APPI Newsletter section 14.
[48] The European Commission has not issued an adequacy certification for Japan, nor has Japan done so for the EU. However, on July 17, 2018, Japan and the EU agreed to complete procedures necessary for an operating framework to facilitate the mutual transfer of personal data between the EU and Japan by the fall of 2018 and have launched internal procedures for the issuance of related mutual adequacy certifications by then.
[49] GDPR, Art. 44-49.
[50] An entity is not a third party for the purposes of the APPI where, for example, it is the same legal entity as the data controller (as determined by the laws of their respective formation) or it is engaged by contract by the data controller to process data for it. Treatment under the GDPR is different, requiring "appropriate safeguards" even if data is transferred within the same corporation.
[51] An opt-out consent cannot be used for special-care-required personal information.
[52] See APPI Newsletter section 6.
[53] See footnote 48.

8. Due Diligence and Transfer Records

Both the APPI and the GDPR have requirements for record-keeping, and the APPI requires due diligence on the transfer of personal information.

GDPR	APPI
A data controller and a data processor must maintain a record of processing activities under their responsibility, and make the record available to the supervisory authority on request.[54]	If a data controller wishes to transfer personal information to a third party, both it and the transferee (if a data controller, or if it becomes a data controller as a result of the transfer) must keep specified records, the transferee also being required to make enquiries on the source of the personal information transferred.[55]

9. Reporting Data Losses

The GDPR data loss reporting regime sets specific deadlines and requirements, whilst the regime established as a consequence of the APPI is very general in nature and it is likely that the procedures for handling of any material data losses in Japan will need to be discussed with the Personal Information Protection Commission.[56]

GDPR	APPI
A data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, provide notice of a personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[57] When a personal data breach is likely to result in a high risk of a negative effect on the rights and freedoms of natural persons, the data	Whilst the APPI does not have provisions dealing directly with reporting of data breaches, provisions do exist in guidelines based on the APPI.[59] The new regime provides that it is "desirable" that a data controller should, in principle, strive to promptly report such incidents to the Personal Information Protection Commission, and promptly inform data subjects who may be affected.[60]

[54] GDPR, Art. 30.
[55] APPI, Art. 25 and 26. See APPI Newsletter section 4.
[56] The Personal Information Protection Commission is an administrative organ established under the APPI for the purpose of ensuring the proper handling of personal information. It is the equivalent of the "supervisory authority" in the GDPR.
[57] GDPR, Art. 33.

controller shall notify the data subject of the personal data breach without undue delay.[58]	

10. Penal Provisions

Both the GDPR and the APPI provide for penalties for breaches of certain of their provisions; the GDPR's potential financial penalties are markedly higher than those under the APPI, though the APPI also provides for liability for imprisonment in certain cases, which the GDPR does not.

GDPR	APPI
Examples of Penalties	
• If a data controller infringes GDPR Art. 8, 11, 25 -39, 42 or 43, e.g. when it fails in its duty to record processing activities, it will be liable to a fine of up to EUR 10,000,000, or if an undertaking, to a fine of up to 2 % of its total worldwide annual turnover of the preceding financial year, whichever is higher. • If a data controller infringes GDPR Art. 5, 6, 7, 9, 12 – 22, 44 – 49, 85 – 91 or 58(2), for instance when it transfers personal data to a third country without an adequacy certification or appropriate safeguards, it will be liable to a fine of up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of its total worldwide annual turnover of the preceding financial year, whichever is higher.[61]	• A data controller which provided or used by stealth personal information that it handled in relation to its business for the purpose of seeking illegal profits for itself or a third party shall be liable to imprisonment for up to one year or to a fine of not more than JPY 500,000. • A person who has breached an order from the Personal Information Protection Commission shall be liable to imprisonment of up to 6 months or a fine of up to JPY 300,000.[62]

[59] "*Regarding responses to leaks of personal data and similar events*" (Personal Information Protection Commission Report, No. 1, 2017)
[60] For further information on the guidelines, please see our Newsletter, "Handling Data Losses: Japan's New Regime" (*http://www.aplaw.jp/news/20180129/*).
[58] GDPR, Art. 34.
[61] GDPR Art. 83.
[62] APPI, Art 83 et seq. See APPI Newsletter section 11 and our newsletter "Handling Data Losses: Japan's New Regime"

CONCLUSION

As can be seen from the analysis above, there are substantial similarities between the data protection regimes under the APPI and the GDPR and it can be hoped that businesses which comply with one regime will not find it unduly burdensome to comply with the other should the need arise.

For further information on these matters, please contact:

Takafumi Uematsu
Attorney (*Bengoshi*), Japan
Partner, Atsumi & Sakai
E: takafumi.uematsu@aplaw.jp

Daisuke Tsuzuki
Attorney (*Bengoshi*), Japan
Associate, Atsumi & Sakai
E: daisuke.tsuzuki@aplaw.jp

Daniel C. Hounslow
Consultant* (UK) to Atsumi & Sakai, Tokyo
E: daniel.hounslow@aplaw.jp

* Mr. Hounslow is a director of Arnaud Advisers Limited (a company incorporated in England and Wales), an independent consultant to Atsumi & Sakai LPC, Tokyo. As such, he is authorised to act for Atsumi & Sakai and in doing so does not act in a personal capacity.

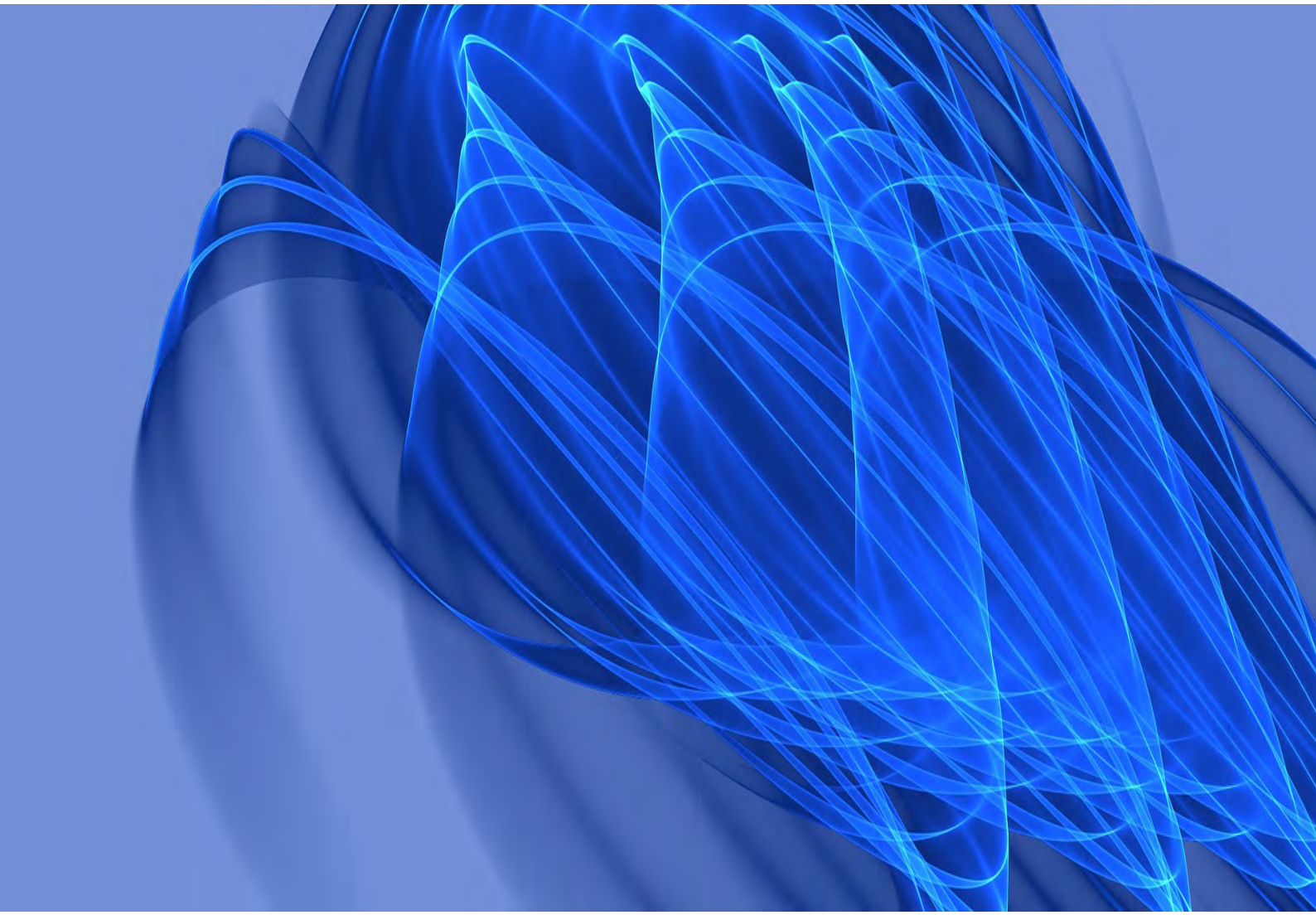
Atsumi & Sakai

www.aplaw.jp

Tokyo Office: Fukoku Seimei Bldg., 2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011, Japan

London Office: 4th Floor, 50 Mark Lane, London EC3R 7QR, United Kingdom

Frankfurt Office: Taunusanlage 21 60325 Frankfurt am Main Germany



www.aplaw.jp/en/