GDR INSIGHT

# HANDBOOK 2021

# HANDBOOK
2021

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com



ISBN: 978-1-83862-266-4

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

# Contents



## Privacy

## Cybersecurity



## Data in practice

# PREFACE

Global Data Review is delighted to publish this second edition of the *GDR Insight Handbook*.

The handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of legislation that a ects how businesses handle their data.

The book's comprehensive format provides in-depth analysis of the global developments in key areas of data law and their implications for multinational businesses. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity. Attention is also given to new legislation in the United States that regulates the use of arti cial intelligence, and strict data localisation rules emerging in jurisdictions such as China. The handbook provides practical guidance on the implications for companies wishing to buy or sell datasets, and the intersection of privacy, data and antitrust. A chapter is dedicated to the use of arti cial intelligence in cross-border forensic investigations.

In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world and we are grateful for all their cooperation and insight.

The information listed is correct as at November 2020. Although every e ort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing eld of practice, and therefore speci c legal advice should always be sought. Subscribers to Global Data Review will receive regular updates on any changes to relevant laws over the coming year.

We would like to thank all those who have worked on the research and production of this publication.

**Global Data Review**
London
*November 2020*

# PART 1

## Privacy

# JAPAN: PRIVACY

Akira Matsuda, Kohei Yamada and Haruno Fukatsu
Iwata Godo

## Key statutes, regulations and adopted international standards

In Japan, data protection regulation for private sector and public sector are separately legislated. We explain below the overview for both sectors, with a focus predominantly on the private sector, which is particularly relevant to this book's readership.

### Rules for business operators in the private sector

#### The Act on the Protection of Personal Information

The Act on the Protection of Personal Information (the APPI) (Act No. 57 of 2003) is the principal legislation in Japan dealing with data protection regulating the private sector. The APPI originally came into force in 2005 and was drastically overhauled in 2017 to take into account rapid technological developments (artificial intelligence, big data, etc) and globalisation, which have brought about new challenges and the increasing need to protect personal data in an environment where the scale of data collection and the sharing of personal data have increased tremendously.

The APPI sets forth obligations imposed on 'business operators' (see 'Foreign groups with an office in Japan'). As the convenient exemption applicable to small and medium-sized enterprises was abolished as part of the 2017 amendments, almost all Japan-based business operators will be covered by the APPI (but not exclusively), regardless of the amount of personal data they are handling or the size of their business (see 'The effect of local laws on foreign businesses').

To clarify and ensure the enforcement of these obligations, the APPI sets forth a basic framework regulating the responsibilities and policies of the national and local governments with regard to the protection of personal information (see 'Regulatory bodies' and 'The effect of local laws on foreign businesses'); establishes the Personal Information Protection Commission (PPC) and defines its roles as the national data protection authority in Japan (see 'Regulatory bodies'); and provides for a set of enforcement measures such as imprisonment or criminal fines.

On 5 June 2020, the bill amending the APPI was passed by the Diet. The amended APPI will come into force in 2022 (see 'Updates and trends').

### Guidelines

The PPC has adopted guidelines to ensure the proper and effective implementation of action to be taken by business operators. The PPC's general guidelines supplement the APPI and separate guidelines apply to specific sectors such as the finance, medical and telecommunications sectors.

### Rules for public-sector organisations

#### Acts covering the protection of personal information in the public sector

Public-sector organisations need to comply with following:

- the Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003); and
- the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc (Act No. 59 of 2003).

### Local regulations

All prefectures and municipal governments in Japan have set forth local regulations on the protection of personal information. The prefectures and municipal governments, and public schools or public hospitals of the prefectures and municipal governments, are covered by these local regulations.

## Regulatory bodies

The PPC is the sole national data protection authority in Japan. The local watchdog was set up as an authority independent from other government bodies. Pursuant to the terms of the APPI, the PPC chairperson and members exercise their judgement and authority independently. The main roles of the PPC are as follows.

- The PPC formulates basic policies on the protection of personal information in accordance with the APPI and promotes the protection of personal information in the public and private sectors. These basic policies include guidelines,[1] which are updated from time to time.
- The PPC has the power to issue guidance and advice, request reports, conduct on-site inspections, make recommendations and issue orders to government institutions and business operators. The range of enforcement measures available is prescribed under article 42 of the APPI.
- The PPC promotes cooperation with data protection authorities in foreign countries through formal and informal exchanges of views with foreign data protection authorities.

1 Guidelines for the Act on the Protection of Personal Information (General Rules); Guidelines for the Act on the Protection of Personal Information (Obligations of Confirmation and Recording at the Time of Provision of Personal Data to Third Parties); Guidelines for the Act on the Protection of Personal Information (Provision to a Third Party in a Foreign Country); Guidelines for the Act on the Protection of Personal Information (Anonymously Processed Information); and Guidelines on Personal Information Protection in the Financial Industry.

- For the purpose of ensuring the proper handling of personal information, the PPC accredits private organisations (ie, accredited personal information protection-organisations) that provide services such as receiving complaints on the handling of personal information, the provision of advice to those making a complaint and the investigation of the circumstances surrounding a complaint based on the APPI. In addition, the PPC supervises these accredited organisations, requiring them to report on the conduct of their services, and may order them to improve their services or take any other necessary action.

## The effect of local laws on foreign businesses

### Foreign groups with an office in Japan

The APPI imposes obligations on business operators handling personal information (ie, business operators). A business operator is defined as 'an entity using a personal information database for use in its business'. Public entities are expressly excluded from this definition. However, there is no similar carve-out for the benefit of companies incorporated in a foreign country or entities having their head office located in a foreign country (ie, a foreign company). This definition reflects the official position of the PPC that the APPI obligations and provisions equally apply to foreign companies if these foreign companies fall under the definition of business operator in Japan. The PPC takes the view that a foreign company is a business operator if it uses a personal information database for its business conducted in Japan, regardless of the place of incorporation or location of the head office.

Therefore, if a foreign company has a branch office or a business office in Japan, or if a foreign company conducts its business in Japan, and uses a personal information database for its business in Japan, this foreign company will fall under the definition of 'business operator'. Furthermore, if a foreign company has a subsidiary in Japan using a personal information database for its business in Japan, this subsidiary falls within the definition of a business operator (although the foreign company itself might not necessarily be covered by the APPI). Accordingly, if a foreign company has an office in Japan, which falls under the definition of 'business operator', regardless of whether such office is branch, business office or subsidiary, APPI-complaint compliance systems must be put in place.

### Foreign groups without an office in Japan

Even if a foreign company has no office in Japan, if this foreign company is collecting personal information from individuals in Japan in connection with a supply of goods or services to these individuals, certain obligations under the APPI would apply to them on an extraterritorial basis. Accordingly, these entities must take measures to comply with these provisions of the APPI.

## Core principles on personal data

The key concepts under the APPI are the following:

- 'Personal information' means information by which a specific living individual is identifiable or information containing an individual identification code (ie, passport number or driver's licence number). Personal information includes information that can be readily combined with other information and make the identification of a specific individual possible.

- 'Personal data' means personal information constituting a personal information database.
- 'Personal information database' means a collective body of information comprising personal information systematically organised to be able to retrieve personal information.
- 'Personal information requiring special care' means sensitive information categorised and defined under the APPI that requires special handling measures, including but not limited to the individual's race, creed, social status, medical history, criminal record, and status as the victim of a crime (ie, sensitive personal information).
- 'Anonymously processed information' means information processed so that such information can no longer be used to identify a specific individual with the necessary safeguards prescribed by the APPI being taken to make it impossible to retrieve personal information.

## Overview of the main obligations under the APPI

The following chart provides a brief outline of the obligations imposed on business operators for each phase during which information is handled.

| Phase | | Type of information | Summary of duties |
|---|---|---|---|
| I | Collection | Personal information | Disclosure of the purpose of use prior to collection of personal information |
| | | | No need to obtain the individual's consent (except for sensitive personal information) |
| II | Utilisation | Personal information and personal data | No need to obtain the individual's consent when utilising within the scope of a previously disclosed purpose of use |
| | | | Duty to take reasonable security measures including preventing the leakage, loss of, or damage to, personal data when handling personal data |
| III | Third-party disclosure | Personal data | **Consent requirement** |
| | | | In principle, individual consent is required for disclosure of personal data to a third party |
| | | | Consent requirement is exempted in case of entrustment of personal data, disclosure upon business succession (ie, M&A), and joint use |
| | | | Regarding joint use, if a business operator informs in advance or ensures that the individual can easily become aware of five statutory elements, the business operator can jointly utilise personal data with a third party, such as a subsidiary, without obtaining any prior individual consent to the disclosure |
| | | | If the business operator meets the opt-out process requirements, there is no need to obtain the individual's consent upon each disclosure of personal data (except for sensitive personal information) |
| | | | **Traceability requirement** |
| | | | An entity disclosing personal data to a third party must keep track (ie, records) of disclosure |
| | | | An entity receiving personal data from a third party must confirm the status of the disclosing party and keep track of disclosure |
| | | | **Cross-border transfer restrictions** |
| | | | In principle, individual consent is required for disclosure to a third party in a foreign country |
| | | | Consent requirement is exempted in those cases described below. |

### Cross-border transfer restrictions

Unless exemption requirements are met, a business operator disclosing personal data to a third party in a foreign country must obtain the individual's prior consent. However, the consent requirement is exempted in the following cases:

- Transfer to a country that is designated by rules of the PPC as a foreign country having established a personal information protection system recognised as being subject to equivalent standards to those applicable in Japan with regard to the protection of an individual's rights and interests (currently, only the European Union is designated as such (effective as of 23 January 2019)).
- The disclosing business operator and the recipient ensure that the recipient develops and implements arrangements through appropriate and reasonable measures for the handling of personal data to be performed consistently with the APPI obligations provisions. These measures may include:
  - contracts between the disclosing business operator and the recipient; or
  - internal rules that are commonly applied to the disclosing business operator and the recipient.
- The recipient receives certification based on the APEC cross-border privacy rules framework (CBPR). The PPC explicitly accepts the APEC-CBPR certification as qualified to meet the standards for 'recognition based on a cross-border privacy rules framework'.

### Overview of the main enforcement measures in the APPI

The main enforcement measures are: imprisonment or criminal fine; an order to cease, desist and take other necessary action to rectify a violation of the APPI against the business operators; or any other action deemed necessary by the PPC within its authority.

## Automated processing, profiling and data analytics

There is currently no regulation specifically restricting automated processing, profiling and data analytics. Under the current interpretation of the APPI, even if information that is equivalent to sensitive personal information is generated or presumed as a result of profiling, this information does not qualify as sensitive personal information under the APPI.

In addition, a business operator handling anonymously processed information is not allowed to collate this information with other information to identify an individual to whom the anonymously processed information relates under the APPI. However, if a business operator identifies a certain individual as a result of profiling using anonymously processed information, this business operator is not considered to have collated anonymously processed information with other information to identify an individual to whom the anonymously processed information relates.

As part of the triennial review of the APPI, there were discussions on whether rules specifically restricting automated processing, profiling and data analytics should be covered in the APPI. It was ultimately decided not to cover this in the 2020 amendments. As an alternative to addressing these issues in the APPI, data subjects' rights have been expanded by relaxing the conditions for requiring that use or third-party transfers of their personal data

be suspended, and for deletion of their data. In particular, under the amended APPI, data subjects will be able to make these requests if their rights or legitimate interests are likely to be infringed; while these rights are more limited under the current APPI.

## Communications and marketing

### Telecommunications

Telecommunications businesses are very large-scale businesses involving the public and, given the nature of their business, operators generally handle large amounts of personal information. Accordingly, the Ministry of Internal Affairs and Communications (MIC), acting as supervisory authority for the telecommunications sector, has issued the following guidelines.

#### Guidelines regarding the protection of personal information for the telecommunications sector

These guidelines contain rules that telecommunication business operators should comply with when they collect, use and transfer information such as communications history, information on callers that includes callers' ID and location information (caller information) for telecommunications (phone calls).

#### Guidelines regarding personal information of the caller in caller information notification service

Certain telecommunication business operators provide a service of notifying the caller's information to the receiver of the call (the caller information notification service). Because caller information is treated as personal information, the MIC has adopted the 'Guidelines regarding personal information of the caller in the context of caller information notification services'.

These guidelines contain rules that caller information notification service providers should comply with when they record, use and transfer caller information.

### Other

The MIC has established a working group regarding the handling of information stored in smartphones such as location information and history of communications (smartphone user information) and this working group has published a Smartphone Privacy Initiative paper that reports their conclusions on how smartphone user information should be protected.

The MIC has also established a committee for the review of the handling of location information in the case of emergency. This committee has reviewed how location information should be utilised for accident prevention. This committee has issued a non-binding report on how such information be protected.

### Marketing

The APPI does not restrict the scope of the purpose of use (including use for marketing purposes) as long as the purpose of use has been disclosed to the public (ie, privacy policy on the website) or notified to individuals. E-marketing is also regulated by the Act on Specified Commercial Transactions (Act No. 57 of 1976) and the Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 2002).

#### The Act on Specified Commercial Transactions

Under this act, sellers or service providers can only make advertisement to consumers via email when recipients opt in to receive email; when sellers or service providers send email advertisement with notice of matters regarding contracts (ie, finalisation of an agreement and shipment of goods); or when sellers or service providers send an email advertisement with an email newsletter that is sent with consent from a recipient.

#### The Act on Regulation of Transmission of Specified Electronic Mail

Under this act, senders can only advertise via email when recipients opt in to receive such email; when recipients notify their email address to the sender in writing (for instance, by providing a business card); when recipients have a business relationship with the sender; or when recipients make their email address available on the internet for business purposes.

## Individuals' rights

### Right to request disclosure

A data subject may request disclosure of retained personal data[2] to a business operator that holds such retained personal data. A business operator must disclose the retained personal data without delay in writing when having received such request.[3]

However, the business operator is exempt from disclosing the retained personal data requested pursuant to article 28(1) of the APPI, in whole or in part, if:

- there is a possibility of harming a data subject or a third party's life, body, assets or other rights and interests;
- there is a possibility of seriously interfering with the business operator from running its business properly; or
- the disclosure violates other laws and regulations.

2 Retained personal data is defined as personal data held by a business operator for more than six months (on the other hand, if the personal data is deleted within six months, such personal data does not fall under the retained personal data and the business operator is not required to respond to the data subject's request) (article 2(7) of the APPI). After the amendment of the APPI, that exemption will no longer apply and the personal data will fall under the retained personal data definition regardless of the length of period they are held by a business operator.

3 Articles 28(1)–(2) of the APPI.

### Right to request correction, addition or deletion

A data subject may request a business operator to make a correction, addition or deletion (collectively, correction) in relation to the content of retained personal data when said retained personal data is incorrect.[4] The business operator must conduct a necessary investigation without delay to the extent necessary to achieve a purpose of use and, based on the result thereof, make a correction of the content of the retained personal data when having received the request pursuant to article 29(1) of the APPI.[5]

However, the business operator is exempt from making a correction where a special procedure concerning a correction of the content is prescribed by other laws or regulations.[6]

### Right to request suspension of use, deletion or suspension of third-party transfers

A data subject may request suspension of use, deletion or suspension of third-party transfers (suspension of use) of the retained personal data if that data is handled in violation of article 16 (purpose-of-use limitation) of the APPI, has been acquired in violation of article 17 (proper acquisition) of the APPI, or has been disclosed to a third party in violation of article 23(1) (restriction on disclosure to a third party) or article 24 (restriction on disclosure to a third party in a foreign country) of the APPI.[7] A business operator must suspend the use of the retained personal data to the extent necessary to remedy the violation without delay, following receipt of a request made pursuant to article 30(1) or (3) of the APPI and when it has become clear that there is a reason for the request.[8]

However, the business operator is exempt from suspension of use where a suspension of use of the retained personal data requires a large amount of expenses or other cases where it is difficult to fulfil a suspension of use, and when necessary alternative action is taken to protect the rights and interests of the data subject.[9]

## The role of the data protection officer

The APPI has no provision mandating the appointment of a data protection officer. However, a business operator is required to take necessary and appropriate action for the security control of personal data including preventing the leakage, loss or damage of its handled personal data.[10] In connection with this provision, the PPC Guidelines require a business operator to take security control measures, including the following:

4 Article 29(1) of the APPI.
5 Article 29(2) of the APPI.
6 id.
7 Article 30(1) and (3) of the APPI.
8 Article 30(2) and (4) of the APPI.
9 Article 30(2) and (4) of the APPI.
10 Article 20 of the APPI.

(1) Organisational security control measures: appointing a person responsible for handling personal data, establishing a system to respond to leakage, loss or damage or personal data, and conducting safety audits on systems that manage personal data.
(2) Human security control measures: employee training on the handling of personal data.
(3) Physical security control measures: access control to areas where important personal data is handled, and storage of documents containing personal data in a cabinet that can be locked.
(4) Technical security control measures: for example, installing a firewall on computers connected externally through networks, and putting restrictions on access to systems that handle personal data.

As stated in (1), since the appointment of a person responsible for handling personal data is listed as one example of organisational safety control measures in the PPC Guidelines, it is the prevailing practice in Japan for a business operator to appoint the responsible person whose tasks or roles are similar to that of a data protection officer in many other jurisdictions.

### Procedure for dealing with data protection breaches and the consequences

For inspectors and investigators, the PPC has the power to require a business operator to submit necessary information or materials relating to the handling of personal information or have its officials enter a business office or other necessary places of a business operator, enquire about the handling of personal information, or inspect books, documents and other properties.[11]

As to corrective measures, the PPC has the power to:

- issue guidance or advice against a business operator with regard to handling personal information;[12]
- recommend a business operator to suspend the violation act or take other necessary action to rectify the violation when recognising there is a need to protect an individual's rights and interests in cases where the business operator has violated the various provisions of the APPI; and
- order a business operator to take action in line with the recommendation when recognising that a serious infringement of an individual's rights and interests is imminent in cases where the business operator having received a recommendation pursuant to article 42(1) of the APPI did not take action in line with the recommendation without legitimate ground.[13]

11 Article 40(1) of the APPI. During fiscal year 2018, there were two cases where the PPC investigated the business offices of the business operators and 391 cases where the PPC required business operators to submit information or materials.

12 Article 41 of the APPI. During fiscal year 2018, there were two cases where the PPC issued guidance or advice to business operators.

13 Article 42(2) of the APPI.

A business operator who has violated an order pursuant to article 42(2) shall be subject to imprisonment with labour for not more than six months or a criminal fine of not more than ¥300,000.[14]

## Updates and trends

### Amendment to the APPI

As mentioned above, the APPI was revised in 2020 as a result of the triennial statutory review process provided for under the APPI; this gives the legislature the opportunity to keep up with the rapid pace of innovation and technical change, and deal with the effects of the continuous expansion of the digital world and the ever-increasing volume of data handled by businesses.

The amendments introduce a number of measures that aim to give more rights to data subjects and stricter rules for businesses (tougher restrictions and prohibitions). These measures are summarised as follows:

- relaxed conditions for data subjects to demand suspension of use, deletion, and suspension of third-party transfers;
- data subjects' right to choose their retained personal data disclosure method (and expansion of the scope of data to be disclosed);
- redefining 'retained personal data': suppression of the short-term data exemption for data deleted within six months;[15]
- third-party transfers without consent: stricter opt-out exemption rules;
- mandatory reporting of the leakage of personal data to the PPC and mandatory notification to data subjects (subject to thresholds); and
- the introduction of a new category of 'Personally Referable Information' subject to specific third-party transfer restrictions under certain circumstances.

The amendments also seek to facilitate data usage, extend the extra-territorial scope of the APPI and strengthen penalties.

The amendments will mainly be in force in spring 2022 (although parts will be in force earlier), and publication of the related secondary legislation and guidelines is scheduled as follows:

- winter 2020: public comments for administrative rules and orders;
- spring 2021: announcement of administrative rules and orders; and
- summer 2021: announcement of guidelines and FAQs.

14 Articles 84 and 87 of the APPI.

15 See footnote No.2.

## Surveillance laws

### CCTV

Images of individuals captured by a surveillance camera and facial recognition data obtained from these images fall under personal information if the images or data can be used to identify a specific individual.

In addition, when such images or facial recognition data are stored in a systematically organised manner, they fall under 'personal information database' and are treated as personal data.

Therefore, the regulations under the APPI would apply to the collection, use or transfer of images of individuals captured by a surveillance camera and facial recognition data obtained from those images.

### Email monitoring

Article 21, paragraph 2 of the Constitution of Japan guarantees the secrecy of any means of communications as a basic human right. In accordance with the Constitution of Japan, the Telecommunications Business Act, the Wire Telecommunications Act and the Radio Act in the area of telecommunications contain provisions protecting the secrecy of communications.

For example, the Telecommunications Business Act provides that 'the secrecy of communications being handled by a telecommunications carrier shall not be violated',[16] which prohibits a third party other than originators and recipients from intentionally viewing communications managed by the telecommunications carrier. Any person who violates provisions of the Telecommunications Business Act is subject to criminal punishment. For example, any person who has violated the secrecy of communications handled by a telecommunications carrier shall be punished by imprisonment with labour of not more than two years or a criminal fine of not more than ¥1 million.[17]

Accordingly, private organisations may not conduct email monitoring in principle. If a company investigates employees' emails that are stored on an internal server to investigate misconduct in the company, this investigation may not violate the secrecy of communications or the right of privacy. However, when conducting an investigation, a cautious approach would be to obtain the consent of the data subject, and if this is not possible, it is recommended to obtain proper legal advice.

## Case studies

Benesse Corporation (Benesse) contracted Synform Co Ltd (Synform) for the development and operation of a system to analyse the personal information of Benesse's customers. In 2014, it became known that an employee of a subcontractor of Synform had leaked personal information of multiple Benesse's customers (such as name, gender, date of birth, address, telephone number and email address), and this incident attracted significant attention.

16 Article 4(1).

17 Article 179(1).

Regarding this case, several civil (Japanese-style) class action lawsuits have been filed against Benesse and Synform by customers based on tort, claiming damages for mental suffering. In one of these lawsuits, the Tokyo High Court entered a judgment on 27 June 2019, admitting the liability of Benesse and Synform and ordering them to pay ¥2,000 to each individual plaintiff.

This case demonstrates that it is important to comply with data protection regulations to mitigate risks of dispute. Furthermore, the judgment refers to the fact that Benesse has paid voluntary compensation to each victim (¥500 per person to approximately 35 million people). As a result of such voluntary compensation payment, Benesse recorded a ¥26 billion special loss during such fiscal year, including ¥6 billion to strengthen security controls and ¥20 billion to fund voluntary compensation.

**Akira Matsuda**
Iwata Godo

Akira Matsuda is an attorney-at-law (admitted in Japan and New York) and a partner at Iwata Godo heading the AI/TMT and data protection practice group. He is based in Tokyo and Singapore. His practice focuses on cross-border transactions, including M&A, as well as international disputes (litigation and arbitration), and advice on digital and TMT-related matters. Mr Matsuda regularly advises Japanese and foreign clients on data security issues (Japanese laws, Singapore's Personal Data Protection Act and the EU General Data Protection Regulation) including on the structuring of global compliance systems. He also advises on complicated cross-border corporate investigation matters.

He is a graduate of the University of Tokyo (LLB) and Columbia Law School (LLM).

**Kohei Yamada**
Iwata Godo

Kohei Yamada is a Japanese attorney-at-law and an associate at Iwata Godo. His practice focuses on M&A and corporate law. His diverse corporate practice includes corporate governance and compliance, shareholders' meetings (listed companies), and dispute resolution. Mr Yamada has advised many Japanese and foreign clients on data protection and privacy issues. He graduated from the University of Tokyo (LLB and JD).

**Haruno Fukatsu**
Iwata Godo

Haruno Fukatsu is a Japanese attorney-at-law and an associate at Iwata Godo. Her practice primarily focuses on corporate law including corporate governance and compliance, shareholders' meetings (listed companies), M&A and domestic commercial dispute resolution. Ms Fukatsu is a member of AI/TMT and data protection practice group and has advised many clients on data protection, privacy and cybersecurity issues, including under Japanese laws and the EU General Data Protection Regulation. She graduated from the University of Osaka (LLB) and the University of Kyoto (JD).

IWATA GODO
Established 1902

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with about 80 attorneys and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection.

Marunouchi Building 15F
2-4-1 Marunouchi,
Chiyoda-ku, Tokyo
100-6315, Japan
Tel: +81 3 3214 6205

www.iwatagodo.com/english

**Akira Matsuda**
amatsuda@iwatagodo.com

**Kohei Yamada**
kyamada@iwatagodo.com

**Haruno Fukatsu**
haruno.fukatsu@iwatagodo.com

The GDR Insight Handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

The book's comprehensive format provides in-depth analysis of the developments in key areas of data law. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity, providing practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-266-4