DATA PROTECTION LAWS OF THE WORLD

Japan vs Germany

DLA PIPER

JAPAN

Last modified 1 January 2024

LAW

The Act on the Protection of Personal Information ("**APPI**") regulates privacy protection issues in Japan and the Personal Information Protection Commission ("**PPC** "), a central agency acts as a supervisory governmental organization on issues of privacy protection.

The APPI was originally enacted in 2003 but was amended and the amendments came into force on 30 May 2017. On 5 June 2020, the Japanese Diet approved a bill to further amend the APPI ("**Amended APPI**"). The Amended APPI came into force on April 1, 2022. Also, there was a separate data protection law for public sector. However, the data protection law for public sector was integrated into the APPI and became effective on April 1, 2022 (the data protection law for local governments became effective after April 1, 2023).

GERMANY

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour* " (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Germany has adjusted the German legal framework to the GDPR by passing the new German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "**BDSG**"). The BDSG came into force together with the GDPR

on May 25, 2018. The purpose of the BDSG is especially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data processing requirements under the GDPR. Part 3 of the BDSG implements the Law Enforcement Directive (EU) 2016/680.

Find the English version here.

In addition to the BDSG, there exist a number of data protection rules in area-specific laws, for example those regulating financial trade or the energy sector. As of 1 December 2021, the Telecommunications-Telemedia-Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz* – "**TTDSG**") provides data protection regulations for telecommunication and telemedia providers, which are intended to eliminate a long-standing legal uncertainty about the applicability of the data protection regulations of the German Telecommunications Act (*Telekommunikationsgesetz* – "**TKG**") and the German Telemedia Act (*Telemediengesetz* – "**TMG**") in interaction with the GDPR. The TTDSG also transposes the “cookie consent” requirement under Article 5 (3) ePrivacy Directive into German law.

DEFINITIONS

Definition of Personal Information

Personal Information is information about a living individual which can identify a specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify a specific individual with easy reference to other information. According to the guidelines issued by the PPC, "easy reference to other information" means that a business operator can easily reference other information by a method taken in the ordinary course of business. If a business operator needs to make an inquiry of another business operator to obtain the "other information" and it is difficult for the business operator to do so, such a situation would not be considered an "easy reference to other information".

Personal Information includes any "Personal Identifier Code". A Personal Identifier Code refers to certain types of data specified under a relevant cabinet order of the

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

APPI, and includes biometric data which can identify a specific individual, or data in the form of a certain code uniquely assigned to an individual. Typical examples of such code would be passport numbers or driver's license numbers.

Definition of Sensitive Personal Information

Sensitive information includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against. Obtaining sensitive information generally requires consent from the data subject. Additionally, the "opt out" option (discussed below) is not available for third party transfer for sensitive information- prior consent is basically required from the data subject to transfer the sensitive information to a third party.

Definition of Anonymously Processed Information

"Anonymously Processed Information" refers to any information about individuals from which all personal information (i.e. the information that can identify a specific individual, including any sensitive information) has been removed and such removed personal information cannot be restored by taking appropriate measures specified in the enforcement rules and the relevant PPC guidelines. As noted above, Personal Information includes personal identifier codes, so these must also be removed before information is considered anonymized.

If a business operator has sufficiently anonymized the information, it can be used beyond the purpose of use notified to the data subjects or disclosed to third parties without requiring the consent of the data subjects. However, care must be taken in anonymizing the information before disclosure; a failure to completely sanitize the information could result in the disclosure of Personal Information. Additionally, before disclosing the Anonymously Processed Information to a third party, a business operator must publicly state (likely in its privacy policy) the items of information (for example, gender, birth year and purchase history) included among the Anonymously Processed Information, and the means by which it shares the Anonymously Processed Information.

Definition of Pseudonymously Processed Information

Given the high hurdle of utilizing Anonymously Processed Information, such information has been less utilized than

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are the same as in Article 4 GDPR. Beyond that, the BDSG contains further definitions for 'public bodies of the Federation', 'public bodies of the Länder' and 'private bodies' in Section 2 BDSG. The TTDSG contains definitions for types of data that are specifically related to the provision of telecommunications and telemedia services (so-called inventory data and usage data).

originally expected. The Amended APPI introduces the concept of "Pseudonymously Processed Information", which is the information that is processed so that such information is (i) not able to be used to identify a specific individual; but (ii) is able to be de-crypted by referencing other information. For example, Pseudonymously Processed Information is information in which names, addresses, and other similar such information are replaced with a random string of characters. Unlike normal Personal Information, a business operator can change the utilization purpose of Pseudonymously Processed Information at its own discretion (i.e. a business operator does not need to obtain consents from data subjects to change the utilization purpose). It is expected that business operators may utilize Pseudonymously Processed Information for internal data analytics purposes.

Definition of Personally Referable Information

The Amended APPI defines information which is related to personal matters, but that does not fall under the definition of Personal Information as "Personally Referable Information". The definition of Personally Referable Information is quite vague, but based on the guidelines issued by the PPC, it includes, among other things, a web browsing history collected through the terminal identifier such as cookie information, a person’s age, gender or family makeup that are linked to his / her email address, a person’s purchase history of goods and / or services, a person’s location data, or a person’s area of interest. The handling of Personally Referable Information is not regulated as Personal Information, but prior consent from data subjects would be required to transfer Personally Referable Information in certain circumstances as discussed below.

NATIONAL DATA PROTECTION AUTHORITY

The PPC has been tasked with providing many of the details necessary to interpret and enforce the APPI. The PPC issues guidelines for general rules for handling Personal Information, offshore transfer, confirmation and record requirements upon provision of Personal Information to third parties and creation and handling Anonymously or Pseudonymously Processed Information. The PPC is neutral and independent, and it has the power to enforce the APPI. However, it will only have the right

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the Garante in Italy). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

to perform audits and issue cease and desist orders; it will not have the power to impose administrative fines and criminal penalties.

Personal Information Protection Commission

Kasumigaseki Common Gate West Tower
32nd Floor
3-2-1 Kasumigaseki
Chiyoda-ku Tokyo 100-0013
Japan

Telephone

+81-(0)3-6457-9680

Website

ppc.go.jp

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Germany does not have one central supervisory authority for data protection law but authorities in each of the sixteen German federal states (*Länder*) that are competent for the public and the private sector in the respective state. In addition, there are different supervisory authorities for private broadcasters as well as for public broadcasters and several supervisory authorities for religious communities.

The German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit* – "**BfDI**") is the supervisory authority for all federal public bodies as well as for certain social security institutions; it also supervises telecommunications and postal service providers, insofar as they provide telecommunications or postal services. The BfDI represents Germany in the European Data Protection Board. To ensure that all the supervisory authorities have the same approach, a committee consisting of members of all authorities for the public and the private sector has been established – the 'Data Protection Conference' (*Datenschutzkonferenz* " **DSK**"). The coordination mechanism between the German supervisory authorities for data protection law mirrors the consistency mechanism under the GDPR.

A list with the contact details and websites of most of the supervisory authorities can be found here.

REGISTRATION

Japan does not have a central registration system.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no general requirement in Germany for controllers or processors to register their processing activities with the competent supervisory authority for data protection law; however, a register of data protection officers (DPOs) is maintained.

DATA PROTECTION OFFICERS

There is no specific legal requirement to appoint a data protection officer. However, some guidelines provide that specific directors or employees should be assigned to control Personal Information (e.g. Chief Privacy Officer).

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or

- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single DPO with responsibility for multiple legal entities (Article 37(2)), provided that the DPO is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single DPO).

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37 (6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The threshold to designate a DPO is much lower in the BDSG. The controller and processor has to designate a DPO if they constantly employ as a rule at least 20 persons dealing with the processing of personal data by automated means, Section 38 (1) sentence 1 BDSG. The meaning of ‘automated processing’ is

interpreted broadly by the German Authorities. It basically covers every employee who works with a computer.

If the threshold of 20 persons is not reached, Section 38 (1) sentence 2 BDSG regulates, that a DPO has to be designated in case the controller or processor undertakes processing subject to a data protection impact assessment pursuant to Article 35 GDPR, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

A dismissal protection for the DPO is provided in Section 38 (2) in conjunction with Section 6 (4) BDSG. Where the controller or processor is obliged to appoint a DPO, the dismissal of a DPO, who is an employee, is only permitted in case there are facts which give the employing entity just cause to terminate without notice. After the activity as DPO has ended, a mandatory DPO who is an employee may not be terminated for a year following the end of appointment, unless the employing entity has just cause to terminate without notice.

Additionally, Section 38 (2) in conjunction with Section 6 (5) and (6) BDSG stipulates that the DPO shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless he / she is released from this obligation by the data subject. Also, the DPO has the right to refuse to give evidence under certain conditions.

Moreover, the German supervisory authorities expect that the DPO speaks the language of the competent authority and the data subjects, i.e. German, or at least that instant translation is ensured.

The supervisory authorities maintain a register of DPOs. No fee is charged for registering or updating the details of a DPO.

COLLECTION & PROCESSING

Specifying the Purpose of Use

COLLECTION & PROCESSING

Data Protection Principles

When handling Personal Information, a business operator must specify to the fullest extent possible the purpose of use of the Personal Information ("Purpose of Use"). Once a business operator has specified the Purpose of Use, it must not then make any changes to the said purpose which could reasonably be considered to be beyond the scope of what is duly related to the original Purpose of Use. In addition, when handling Personal Information, a business operator shall not handle the information beyond the scope that is necessary for the achievement of the Purpose of Use without a prior consent of the individual. In other words, the use of the information must be consistent with the stated Purpose of Use.

Public Announcement of the Purpose of Use

The Purpose of Use must be made known to the data subjects when Personal Information is collected or promptly thereafter and this can be made by a public announcement (such as posting the purpose on the business operator's website). When Personal Information is obtained by way of a written contract or other document (including a record made in an electronic or magnetic format, or any other method not recognizable to human senses), the business operator must expressly state the Purpose of Use prior to the collection.

A business operator must 'publicly announce or 'expressly show the Purpose of Use in a reasonable and appropriate way. According to the guidelines issued by the PPC, the appropriate method for a website to publicly announce the Purpose of Use of information collected, is a one click access on the homepage so that the data subject can easily find the Purpose of Use before submitting the Personal Information.

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known as lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;

- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;

- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law

which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12 (1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when the European Union’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “ compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The BDSG has additional rules regarding processing of special categories of personal data. Contrary to Article 9 (1) GDPR, processing of such data is permitted by public and private bodies in some cases which are based on the exceptions in Article 9 (2) GDPR, see Section 22 (1), 26 (3) BDSG. Also, Section 24 BDSG determines cases in which controllers are

permitted to process data for a purpose other than the one for which the data were collected.

Section 4 BDSG provides a special rule for video surveillance of publicly accessible areas. According to the German data protection supervisory authorities as well as the German Federal Administrative Court (*Bundesverwaltungsgericht* – "**BVerwG**") and the near unanimous opinion in German legal literature, the provision is not compliant with the GDPR insofar as it regulates surveillance by private bodies (Section 4 (1) Nos. 2, 3 BDSG). This is based on the argument that the GDPR does not contain any opening clause on which these deviations from Article 6 (1) GDPR could be based.

Furthermore, the BDSG provides special rules regarding processing for employment-related purposes in Section 26 BDSG. The German legislator has made very broad use of the opening clause in Article 88 (1) GDPR and has basically established a specific employee data protection regime, that mostly only repeats the general legal bases of performance of contract respectively “*carrying out the obligations and exercising specific rights… in the field of employment and social security and social protection law*” (Art. 9(2)(b) GDPR). Due to this, the European Court of Justice ruled that a provision in German state data protection law (which applies to the public sector) that corresponds with the “ performance of the employment contract” legal basis in Section 26 BDSG is invalid (Judgment of the CJEU in Case C-34/21). This is because the law failed to establish specific provisions, although this is a requirement pursuant Article 88(1) GDPR for national legal bases. Due to this decision, it is widely assumed (including by the German supervisory authorities that (some) of the respective German legal bases for the processing of employee personal data in the BDSG are invalid.

Employers should therefore rely (alternatively or additionally) on the GDPR legal bases for the processing of employee and candidate personal data for the establishment or the performance of the employment contract (Article 6(1)(b) GDPR) respectively on Article 9(2)(b) GDPR. In particular when determining what is “ necessary” for the performance of the

employment contract, employers also need to comply with the case law of the German Federal Labour Court (*Bundesarbeitsgericht* – "**BAG**").

In addition, there is a legal basis specifically for the investigation of criminal offences against employees which likely is still valid.

Furthermore, processing of employee personal data for purposes that are not specifically related to employment as such can still be based on Article 6 (1) GDPR. In particular, controllers that are part of a group of companies may be able to base transfers of data within the group for internal administrative purposes on their legitimate interests in accordance with to Article 6 (1) f) (as stated by Recital 48 of the GDPR).

The processing of personal data in the context of the provision of telecommunication services is subject to Section 9 et seqq. TTDSG. Furthermore, both the content of telecommunications and its detailed circumstances, in particular the fact whether someone is or was involved in a telecommunications process, is subject to the secrecy of telecommunications, Section 3 TTDSG. Violations of the secrecy of telecommunications constitutes a criminal offence under the German Criminal Code (*Strafgesetzbuch* – "**StGB**").

The processing of personal data in the context of the provision of telemedia (like for example a website or a social network) is subject to specific limitations contained in Section 19 et seqq. TTDSG. There are, inter alia, specific requirements regarding the provision of inventory data, passwords or usage data to public authorities in Section 22 et seqq. TTDSG.

The following German specific rules for the processing of personal data in the employment context likely are still valid:

- Employees’ personal data may be processed to detect criminal offenses only if there is a documented reason to believe the data subject has committed such an offense while employed, the processing of such data is necessary to investigate the offense and is not outweighed by the data subject’s

legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason (Section 26 (1) sentence 2 BDSG) (this blocks investigation based on legitimate interests pursuant Article 6(1) f GDPR);

- The processing is based on a works council agreement which complies with the requirements set out Article 88 (2) GDPR (Section 26 (4) BDSG);
- The processing is based on the employee’s consent in written or electronic form. A derogation from this form can apply if a different form is appropriate because of special circumstances (but this derogation will rarely apply in practice). Moreover, the utilization of consent as basis for the processing is particularly problematic in Germany as Section 26 (2) BDSG stipulates requirements in addition to Article 7 GDPR. If personal data of employees are processed on the basis of consent, then the employee’s level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. The German data protection supervisory authorities interpret this provision in a way that employee consent cannot be used for processing of personal data which directly relates to the employment relationship, but only to supplementary services offered by the employer (e.g. private use of company cars or IT equipment, occupational health management or birthday lists).

TRANSFER

Disclosing / Sharing Personal Information

TRANSFER

Currently, Personal Data (meaning Personal Information stored in a database) may not be disclosed to a third party without the prior consent of the individual, unless the business operator handling the Personal Information adopts the opt-out method, provides an advance notice of joint use to data subjects, in the case of merger / business transfer or entrusting the handling of Personal Information to third party service providers.

Even disclosing the Personal Information within group companies is considered disclosing the Personal Information to a third party and consent must be obtained, unless it meets the requirements of joint use. The APPI also has permitted the "opt out" method, whereby a business operator can as a default disclose Personal Information to third parties, unless individuals opt out of allowing the business operator to do so. The Amended APPI stipulates that Personal Information that has been transferred from others through the opt out measure or that has obtained by illegal manners, and Sensitive Personal Information cannot be transferred through the opt out measure. The APPI requires a business operator to preemptively disclose to the PPC, and the public or to the data subject of certain items listed below concerning opt out.

- the name, address and representative person of the business operator;
- the fact that the purpose of use includes the provision of such information to third parties;
- the nature of the Personal Information being provided to third parties;
- the method by which Personal Information has been obtained;
- the method by which Personal Information will be provided to third parties;
- the matter that provision of such information to third parties will be stopped upon the request by the data subject;
- the method for an individual to submit an opt out request to the business operator;
- the method to update Personal Information which has been provided to their parties; and
- the schedule date of provision of Personal Information.

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on the condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing Personal Information. Generally, written consent should be obtained whenever possible. When obtaining consents, it would be prudent to clearly disclose to the data subject the identity of the third party to whom the Personal Information will be disclosed, the contents of the Personal Information and how the third party will use the provided Personal Information.

The guidelines issued by the PPC provide the following examples as appropriate methods of obtaining the consent for disclosing Personal Information from the data subject:

- receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from data subject;
- receipt of a consent email from data subjects;
- the data subject's check of the confirmation box concerning the consent;
- the data subject's click of a button on the website concerning the consent; and
- the data subject's audio input, or touch of a touch panel concerning the consents.

If Personal Information is to be used jointly, the business operator could, prior to the joint use, notify the data subjects of or publish the following:

- the fact that the Personal Information will be used jointly;
- the item of the Personal Information to be disclosed;
- the scope of the joint users;
- the purpose for which the Personal Information will be used by them; and
- the name, address and representative person of the business operator responsible for the management of the Personal Information.

Transfer of Personally Referable Information

The Amended APPI stipulates that prior consent from data subjects is necessary if Personally Referable Information is transferred to a third party and the receiving party can identify a specific individual by way of referencing such Personally Referable Information with any information that the receiving party already has in its possession. In general, such consents are to be obtained by the receiving party and therefore, the transferor needs

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The transfer of personal data to a third country or to supranational or intergovernmental bodies or international organisations in the context of activities not falling within the scope of the GDPR or the Law Enforcement Directive (EU) 2016/680 are also permitted if they are necessary for the performance of own tasks for imperative reasons of defence or for the performance of supranational or intergovernmental obligations of a federal public body in the field of crisis management or conflict prevention or for humanitarian measures.

For more information, please visit our Transfer - global data transfer methodology website.

to, in advance to transferring Personally Referable Information to a third party, confirm if the receiving party has already obtained consents. That being said, it is possible that the transferor collects data subjects’ consents on behalf of the receiving party.

Cross-border Transfer

Under the APPI, in addition to the general requirements for third party transfer, prior consent of data subjects specifying the receiving country is required for transfers to third parties in foreign countries unless the foreign country is white-listed under the enforcement rules of the APPI or the third party receiving Personal Information has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI. Currently, UK and EU countries are specified as white-listed countries based on the adequacy decision on January 23, 2019.

According to the enforcement rules of the APPI, "similarly adequate standards" means that the practices of the business operator handling the Personal Information are at least equal with the requirements for protection of Personal Information under the APPI or that the business operator has obtained recognition based on international frameworks concerning the handling of Personal Information.

According to the guidelines for offshore transfer, one of the examples of an acceptable international framework is the APEC CBPR system. With regard to data subject's consents to transfer their Personal Information to foreign countries, the Amended APPI stipulates that the business operator shall provide the following information to the data subject when obtaining consents therefrom: (i) name of the country where the receiving party resides, (ii) data protection law system in the country and (iii) the data protection measures that the receiving party implements. In addition, the business operator needs to take necessary measures to ensure that the receiving party of such Personal Information continuously takes proper measures to process the Personal Information in a manners equivalent to the requirements of the APPI.

SECURITY

The APPI requires that business operators prevent the leakage of Personal Information. The APPI does not set forth specific steps that must be taken. The PPC guidelines suggest recommended steps that business operators should take to ensure that Personal

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security.

Information is secure. These necessary and appropriate measures generally include "Systematic Security Control Measures", "Human Security Control Measures", "Physical Security Measures" and "Technical Security Control Measures".

Guidelines often contain several specific steps or examples that entities subject to the guidelines must take with respect to each of the security control measures such as developing internal guidelines pertaining to security measures, executing non-disclosure contracts with employees who have access to Personal Information, protecting machines and devices and developing a framework to respond to instances of leakage.

Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The BDSG has additional rules regarding the processing of special categories of personal data in Sec. 22 (2) BDSG. In case of processing of such data, appropriate and specific measures have to be taken to safeguard the interests of the data subject.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

- technical and organizational measures to ensure that processing complies with the GDPR;
- measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
- measures to increase awareness of staff involved in processing operations;
- designation of a data protection officer;

- restrictions on access to personal data within the controller and by processors;
- the pseudonymization of personal data;
- the encryption of personal data;
- measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
- specific rules of procedure to ensure compliance with this Act and with the GDPR in the event of transfer or processing for other purposes.

BREACH NOTIFICATION

Under the Amended APPI, business operators shall report data breach incidents to the PPC and affected data subjects if the data breach incidents could harm the rights and interests of individuals. The PPC set the concrete threshold for reporting obligations and in the case of any of the below (i)-(iv), the business operator needs to report it to the PPC and notify the affected individuals: (i) Sensitive Personal Information is or likely to have been leaked, (ii) Personal Information that would cause financial damage by unauthorized use is or likely to have been leaked, (iii) data leakage by wrongful purpose is or likely to have been occurred, and (iv) data leakage incident that involves more than 1,000 data subjects is or likely to have been occurred.

In addition, the PPC guidelines suggest that business operators (i) make necessary investigations and take any necessary preventive measures, and / or (ii) make public the nature of the breach and steps taken to rectify the problem, if appropriate and necessary.

According to the PPC guidelines, if a factual situation demonstrates that the Personal Information which has been disclosed was immediately collected before being seen by any third party or not actually disclosed, (such as the case where the company has encrypted the data or otherwise secured the data in such a way that it has become useless to third parties being in possession of

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

such data), the notice to the PPC or any other relevant authority is not necessary.

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to the competent supervisory authority. The German supervisory authorities generally make available specific web forms for notifications and some of them have published risk rating requirements for personal data breach notifications.

The German BDSG only contains slight changes and additions to the regulations in Article 33, 34 GDPR.

Section 29 (1) BDSG stipulates in addition to the exception in Article 34 (3) GDPR, the obligation to inform the data subject of a personal data breach according to Article 34 GDPR shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from this, the data subject pursuant to Article 34 GDPR shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

According to Section 43 (4) BDSG, a notification pursuant to Article 33 GDPR or a communication pursuant to Article 34 (1) GDPR may be used in proceedings pursuant to the Act on Regulatory Offences (*Gesetz über Ordnungswidrigkeiten –* "**OWiG**") against the person required to provide a notification or a communication only with the consent of the person obligated to provide a notification or a communication.

ENFORCEMENT

If the PPC finds any violation or potential violation of the APPI, the PPC may request the business operator to submit a report, conduct on-site inspection and request or order the business operator to take remedial actions. If a business operator does not submit the report and materials, or reports false information they will be subject to a fine of up to JPY 500,000.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

If a business operator does not follow an order from the PPC they will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 1,000,000. If the party that fails to follow such order is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

An unauthorized disclosure of Personal Information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 500,000. If the party that discloses Personal Information is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘ undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘ undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In October 2019 the German data protection authorities published guidelines for calculating administrative fines against ‘business undertakings’ under Article 83 GDPR. However, since the final version of the Guidelines 04/2022 on the calculation of administrative fines under the GDPR of the EDPB was adopted in May 2023, the German guidelines are no longer relevant.

Enforcement powers

There are no German specific enforcement powers except for the German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit* – "**BfDI** ") competent for federal authorities and certain sectors (see Authority for details).

Administrative powers

German law provides for administrative fines of up to 50,000 EUR for the violation of German specific requirements for the processing of personal data in the context of consumer loans (Sections 30 and 43 BDSG).

Criminal offences

The BDSG provides for several offences which can result in prosecution of, imprisonment, and criminal penalties being imposed of / on individuals. The offences under the BDSG include:

- transferring personal data to a third party or otherwise making them accessible if done deliberately and without authorization for commercial purposes and with regard to the personal data of a large number of people which are not publicly accessible;
- processing without authorization, or fraudulently acquiring, personal data which are not publicly accessible if doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

Additionally other special laws provide for criminal offences (e.g. violations of the secrecy of telecommunications constitutes a criminal offence under the German Criminal Code (*Strafgesetzbuch* – StGB)).

ELECTRONIC MARKETING

The Act on Specified Commercial Transactions ("**ASCT** ") and the Act on the Regulation of Transmission of Specified Electronic Mail ("**Anti-Spam Act**") regulate the sending of unsolicited electronic commercial communications.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the

Under the ASCT, which focuses on internet-order services, a seller is prohibited from sending email or fax advertisements to consumers unless they provide a prior request or consent (i.e. an opt-in requirement). The seller is also required to retain the records that show consumers' requests or consents to receive email or fax advertisements for 3 years for email advertisements and 1 year for fax advertisements after the last transmission date of an email or fax advertisement to the consumer.

If a seller has breached any of these obligations regarding email advertisements, such seller will be potentially subject to fine of up to JPY 1,000,000.

Under the Anti-Spam Act, which broadly covers commercial emails (e.g. an invitation email from a social network service), there are several regulations on sending email advertisements as follows:

- the sender must retain records evidencing there was a request or consent to receive emails at least for 1 month after the last date the seller sent an email to the recipient;
- for-profit entities or individuals engaged in business sending any email to advertise their own or another’s business must obtain a request or consent to receive emails from intended recipients unless the recipient falls under certain exceptions (e.g. there is a continuous transaction relationship between a sender and a recipient) in the Anti-Spam Act;
- an email is required to include a sender’s email address or a URL so that recipients can send opt-out notices to the sender; and
- senders must not send emails to randomly generated email addresses (with the hope of hitting an actual email address) for the purpose of sending emails to a large number of recipients.

The relevant ministry may order a sender to improve the manner of email distribution if the sender violates the requirements noted above. If the sender violates an order issued by the ministry (other than one related to the retention obligation), the sender is subject to imprisonment for up to 1 year or a fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 30,000,000 if an officer or an employee of the entity commits any violation mentioned above. If the sender violates an order issued by the minister with respect to the retention obligation, the sender will be

controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is likely to be replaced by a regulation (the so called ePrivacy Regulation), but it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the ‘same service / product’ exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt-out prior to the first marketing email
- the user did not opt-out, and
- the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

potentially subject to fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 1,000,000 if an officer or an employee of the entity commits the violation mentioned above.

Like the GDPR, the German BDSG also does not provide for any specific provisions regarding marketing. The use of electronic communication for the purpose of direct marketing as currently regulated in ePrivacy Directive has been transposed into German law and is implemented in Section 7 of the German Act Against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb* – "**UWG**") As emphasized by the German Authorities (in their guidelines on direct marketing), processing of personal data for the purpose of marketing communication which is in breach of Section 7 UWG also constitutes a breach of the GDPR as it does not follow a legitimate purpose.

When using electronic communication for direct marketing, prior consent is generally required, cf. Section 7 (2) no. 1, 2 UWG, the standard for this being the so-called double opt-in process. According to Article 6 (1) a) GDPR as well as according to established German case law, data subjects must always give consent for a specific processing purpose. This means that the person to be contacted needs to know (1) from whom (meaning which specific entity or entities), (2) for which specific products and services he / she will receive marketing offers and (3) by which means (e.g. email or telephone).

The German lawmaker has also transposed the ‘same service / product’ exemption into Section 7 UWG. Based on Section 7 (3) UWG, direct marketing can be based on the exemption if the following prerequisites are met:

- the recipients electronic mail address was obtained from the sender in connection with the sale of goods or services;
- the sender uses the address for direct advertising of his own similar goods or services (no cross-selling permitted);
- the recipient has not objected to this use; and
- the recipient is clearly and unequivocally advised, upon the collection of the address as well as each time it is used, that he or she can object to such use at any time, without costs arising by virtue thereof, other than transmission costs pursuant to the basic rates.

ONLINE PRIVACY

There is no law in Japan that specifically addresses cookies, but it is generally considered that cookies fall under the definition of the Personally Referable Information and thus the transfer of such data would be regulated by the APPI in certain circumstances. In addition, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (e.g. member registration) and it is utilized (e.g. for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the **APPI**.

Moreover, under the Telecommunications Business Act, when providing telecommunications services to users as specified in the applicable Ministry of Internal Affairs and Communications ordinance and sending a telecommunication to the user’s device that gives a command to activate the device's information transmission function which transfers the information to third parties (such as third-party cookie), the service provider must take one of the following measures: (i) notify users of the content of information to be sent, Purpose of Use and the destination of information to be sent, or put these information in a condition where users can easily learn about it, (ii) obtain users consent, or (iii) take opt-out measures.

ONLINE PRIVACY

The General Data Protection Regulation (GDPR) supersedes national data protection law unless there is an opening clause constituted under GDPR. Due to Article 95 GDPR this is the case for national data protection law that was created to implement the Directive on privacy and electronic communication (Directive 2002/58/EC; "ePrivacy Directive").

The German legislator created national data protection regulations for providers of telecommunication services and for providers of certain electronic information and communication services (e.g. website operators) within the TTDSG, which was adopted on 1 December 2021. The TTDSG aims to eliminate the legal uncertainties caused by the fact that special data protection provisions were previously regulated in two different laws, the TKG and the TMG, which were both not adapted to the GDPR. As a result, in the past German data protection authorities and courts sometimes disagreed on which of these provisions, if any, were applicable.

The TTDSG eliminates some provisions that were deemed unapplicable and shifts the data protection regulations regarding telecommunication and telemedia into a single law, which stands alongside the GDPR and the BDSG. The TKG and the TMG have been amended and remain effective, but no longer contain data protection regulations. Whether this new legislation will actually put an end to the previous discussions remains to be seen.

Cookie compliance

The legal requirements with regard to the use of cookies were long unclear in Germany. It was disputed whether there was any consent requirement for cookies at all, as the respective provisions of the ePrivacy Directive had never been transposed into German law (which was also the opinion of the German data protection authorities at that time). Cookie consent was then required as of 28 May 2020, when the German Federal Court of Justice (*Bundesgerichtshof* – "**BGH**") ruled that Section 15 (3) TMG (which technically only provides for an opt-out requirement regarding the use of cookies) was to be construed as a requirement for cookie consent in the meaning of the ePrivacy Directive.

With Section 25 TTDSG, Germany finally transposed Article 5 (3) of the ePrivacy Directice into national law in

December 2021, making cookie consent a legal obligation while explicitly including the definition of consent in terms of the GDPR.

In accordance with the ePrivacy Directive, under German law consent is not required where the sole purpose of cookies (or to be more precise, of the storage of information or access to information already stored in the users terminal equipment) is carrying out the transmission of a communication over a public telecommunications network or providing a telemedia service explicitly requested by a user (Section 25 (2) TTDSG).

In addition to that, the German data protection authorities have long been of the opinion that the processing of personal data enabled by the cookies used for analysis and tracking tools regularly requires consent, in particular if the tools allow third parties to collect data from website users as (joint) controllers. It remains to be seen whether this position will be upheld by the BGH or another superior German court.

Traffic data

Lawful processing of traffic data is governed by Section 9 et. seqq. TTDSG and may only take place to the extent it is necessary for the purposes constituted therein or if other legal provisions require a processing. Those who provide or participate in the provision of telecommunication services have to take the technical precautions and actions necessary to protect personal data in accordance with Section 165 TKG; in this context the state of the art must be observed. In addition, the service providers are required to protect the secrecy of telecommunications, which extends to both the content of telecommunications and its detailed circumstances, in particular the fact whether someone is or was involved in a telecommunications process.

Providers of telecommunication services in terms of Section 3 (2) sentence 1 TTDSG may process traffic data for the establishment and maintaining of a telecommunications connection, remuneration inquiry and billing, fraud prevention as well as detection and remedy of disruptions regarding telecommunications systems and tracing of malicious or nuisance calls. Processing of traffic data for marketing purposes, need-based design of telecommunication services and provision of value-added services requires consent in accordance with GDPR.

Generally, traffic data shall be deleted by the service provider without undue delay after termination of each

telecommunications connection or as soon as the data are no longer necessary in relation to the purpose for which they are otherwise being processed. However, data may and must be stored in case statutory retention periods under the TTDSG, TKG or other law apply.

If there is a particular and significant risk of a security incident, providers of publicly available telecommunication services shall notify the users about any possible protective or remedial measures that can be taken by users and, where appropriate, about the threat itself (Section 168 (6) TKG), in addition to their general notification obligations with respect to security incidents towards the German Federal Network Agency (*Bundesnetzagentur* – "**BNetzA**") and the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – "**BSI**").

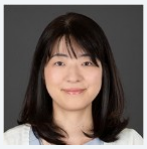
Location data

Publicly available telecommunication services may only process location data for the purpose of providing value-added services in case the data are rendered anonymous or processing is based on consent in terms of the GDPR (Section 13 (1) TTDSG).

Consent can be withdrawn at any time and where consent was given to the processing of location data, it must be possible, by simple means and free of charge, to temporarily prohibit the processing of such data for each connection to the network or for each transmission of a message.

The processing of location data in other contexts than telecommunication services (like for example GPS tracking) is subject to the GDPR.

KEY CONTACTS



Tomomi Fujikouge
Of Counsel
T +81 3 4550 2817
tomomi.fujikouge@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KEY CONTACTS

Verena Grentzenberg
Partner
T +49 40 188 88 203
verena.grentzenberg@dlapiper.com

Dr. Jan Geert Meents
Partner
T +49 89 23 23 72 130
jan.meents@dlapiper.com

Jan Pohle
Partner
T +49 221 277 277 391

jan.pohle@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.