DATA PROTECTION LAWS OF THE WORLD

Australia vs Germany

DLA PIPER

AUSTRALIA

Last modified 31 December 2023

LAW

Australia regulates data privacy and protection through a mix of federal, state and territory laws. The federal Privacy Act 1988 (*Cth*) ("**Privacy Act**") and the Australian Privacy Principles ("**APPs**") contained in the Privacy Act apply to private sector entities (including body corporates, partnerships, trusts and unincorporated associations) with an annual turnover of at least AU$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies.

The Privacy Act regulates the handling of personal information by relevant entities and under the Privacy Act, the Information Commissioner has authority to conduct investigations, including own motion investigations, to enforce the Privacy Act and seek civil penalties for serious and egregious breaches or for repeated breaches of the APPs where an entity has failed to implement remedial efforts.

The Privacy Act is currently undergoing a review and the Attorney General’s Department released the Privacy Act Review Report 2022 setting out 116 proposed amendments to the Privacy Act. The Government Response to the Privacy Act Review Report released in 2023 indicated that of the 116 recommendations, the Australian Government “ agreed” to 38 of them, “agreed in principle” to another 68 and rejected 10. The timing for the implementation of these changes is not yet clear, however, it is likely that this will be undertaken during 2024 – 2025 and that any revisions will result in more prescriptive and onerous requirements being imposed on organisations handling personal information of Australian residents.

In late 2023, appointments were made of a separate Privacy Commissioner and Freedom of Information Commissioner - these roles were all performed by the Information Commissioner. The Privacy Commissioner

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

will perform the privacy functions which relate to the privacy of individuals with both new appointments beginning in February 2024.

Most States and Territories in Australia (except Western Australia and South Australia) have their own data protection legislation applicable to relevant State or Territory government agencies, and private businesses that interact with State and Territory government agencies. These Acts include:

- *Information Privacy Act 2014* (Australian Capital Territory)
- *Information Act 2002* (Northern Territory)
- *Privacy and Personal Information Protection Act 1998* (New South Wales)
- *Information Privacy Act 2009* (Queensland)
- *Personal Information Protection Act 2004* (Tasmania), and
- *Privacy and Data Protection Act 2014* (Victoria)

Additionally, there are other parts of State, Territory and federal legislation that relate to data protection. For example, the following all impact privacy and data protection for specific types of data or activities: the *Telecommunications Act 1997* (*Cth*), the *Criminal Code Act 1995* (*Cth*), the *National Health Act 1953* (*Cth*), the *Health Records and Information Privacy Act 2002* (NSW), the *Health Records Act 2001* (Vic) and the *Workplace Surveillance Act 2005* (NSW).

Specific regulators have also expressed an expectation that regulated entities should have specified data protection practices in place. For example, the Australian Prudential and Regulatory Authority ("**APRA**"), which regulates financial services institutions requires regulated entities to comply with Prudential Standards, including Prudential Standard CPS 234 Information Security ("**CPS 234**"), and the Australian Securities and Investment Commission regulates corporations more generally.

Other important privacy and data protection laws

Assistance and Access Act

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* ("**AA Act**") provides law enforcement agencies with access to encrypted data for serious crime investigation and

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.

imposes obligations on "Designated Communications Providers". However, the AA Act may inadvertently have a much broader remit with limited judicial oversight, and has been the subject of much criticism from local and global technology firms which have stated the legislation has the potential to significantly impact security / encryption solutions in Australia.

The AA Act allows various agencies to do any of the following:

- Issue a "technical assistance notice", which requires a communications provider to give assistance that is reasonable, proportionate, practicable and technically feasible;
- Issue a "technical capability notice", which requires a communications provider to build new capabilities to assist the agency. The Attorney-General must consult with the communications provider prior to issuing the notice, and must be satisfied that the notice is reasonable, proportionate, practicable and technically feasible; and
- Make "technical assistance requests", to give foreign and domestic communications providers and device manufacturers a legal basis to provide voluntary assistance to various Australian intelligence organizations and interception agencies relating to issues of national interest, national security and law enforcement.

Organizations will need to ensure customer terms and conditions deal carefully with the matter of legal compliance and any commitments made to customers generally.

Security of Critical Infrastructure Act

The *Security of Critical Infrastructure Act 2018 (Cth)* ("**SOCI Act**") applies to organisations that own or operate (or hold a direct interest in) assets in a range of sectors including communications, energy, defence, financial services, transport, data processing or storage, supermarket / grocery supply chains, health and medical, education and space.

The key obligations under the SOCI Act include:

- Organisations must provide “ operational” and ownership information to the Cyber Infrastructure Security Centre for inclusion on the Register of Critical Infrastructure Assets, in accordance with the requirements in Part 2 of the SOCI Act;

- Organisations must notify the Australian Signals Directorate ("**ASD**") of actual or imminent cyber security incidents with an actual or likely relevant impact within 72 hours of the organisation becoming aware, in accordance with the requirements set out in Part 2B of the SOCI Act; and
- Organisations must implement and comply with a "risk management program", in accordance with the requirements in Part 2A of the SOCI Act and the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.

Generally, organisations to whom the SOCI Act applies or those that provide services to relevant organisations should ensure that any terms and conditions deal with compliance with the obligations under the SOCI Act.

Consumer Data Right

The Commonwealth Government is in the implementation phases of the Consumer Data Right (“**CDR**”) following a number of policy reviews including the Productivity Commission's "Data Availability and Use" report and the "Review into Open Banking in Australia".

The CDR allows a consumer to obtain certain data held about that consumer by a third party and require data to be given to accredited third parties for certain purposes. By requiring businesses to provide public access to information on specified products they have on offer, it is intended that consumers' ability to compare and switch between products and services will be improved, as well as encouraging competition between service providers, which could lead to better prices for customers and more innovative products and services. In this way, the CDR provides a mechanism for accessing a broader range of information within designated sectors than is provided for by APP 12 in the Privacy Act, given it applies not only to data about individual consumers but also to business consumers and related products.

The CDR rules have been implemented in respect of the banking and energy sector in Australia. The non-bank lending sector is the next to be added to the CDR. Other sectors across the economy will be added to the CDR over time.

The CDR regime addresses competition, consumer, privacy and confidentiality issues. As such, it is regulated by the Australian Competition and Consumer Commission as well as the OAIC.

DEFINITIONS

Definition of personal data

Personal data (referred to as "personal information" in Australia) means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not.

The Privacy Act currently contains an exemption for “employee records”, such that any records containing personal information which an employer makes in connection with a current or former employment relationship are exempt from the Privacy Act. However there are some further carve outs to this (for example, the exemption does not apply to contractors or unsuccessful applicants), and it is widely anticipated that the employee records exemption will be removed from the Privacy Act as a result of the ongoing review of the Privacy Act (see Enforcement).

Definition of sensitive personal data

Sensitive personal data (referred to as "sensitive information" in Australia) means information or an opinion about:

- Racial or ethnic origin;
- Political opinions;
- Membership of a political association;
- Religious beliefs or affiliations;
- Philosophical beliefs;
- Membership of a professional or trade association;
- Membership of a trade union;
- Sexual orientation or practices;
- Criminal record that is also personal information;
- Health information about an individual;
- Genetic information about an individual that is not otherwise health information;

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).

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

- Biometric information that is to be used for the purpose of automated biometric identification or verification; and / or

- Biometric templates.

NATIONAL DATA PROTECTION AUTHORITY

The Information Commissioner, under the Office of the Australian Information Commissioner ("**OAIC**") is the national data protection regulator responsible for Privacy Act oversight.

175 Pitt Street
Sydney NSW 2000

T 1300 363 992

F +61 2 9284 9666

related to the provision of telecommunications and telemedia services (so-called inventory data and usage data).

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.

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

There is no registration requirement in Australia for data controllers or data processing activities. Under the Privacy Act, organizations are not required to notify the Information Commissioner of any processing of personal information.

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

Organizations are not required to appoint a data protection officer. However, the Information Commissioner has issued guidance recommending that organizations appoint a data protection officer as good practice.

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

Organizations may not collect personal information unless the information is reasonably necessary for one or more of its business functions or activities.

Under the Privacy Act, organizations must take reasonable steps to ensure that personal information collected is accurate and up-to-date.

At or before the time organizations collect personal information, or as soon as practicable afterwards, they must take reasonable steps to provide individuals with notice of:

- The Organization’s identity and contact information;
- Why it is collecting (or how it will use the) information about the individual;
- The entities or types of entities to which it might give the personal information;
- Any law requiring the collection of personal information;
- The main consequences (if any) for the individual if all or part of the information is not provided;
- The fact that the organization’s privacy policy contains information about how the individual may access and seek correction of their personal information, how they may make a complaint about a breach of the APPs and how the organization will deal with such complaint; and

COLLECTION & PROCESSING

Data Protection Principles

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

- Whether the organization is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

Organizations should comply with these notification requirements by preparing a “collection statement” or “privacy notice” for each significant collection of personal information, and providing this to individuals prior to collecting their personal information.

This notification requirement applies in addition to the requirement for organisations to maintain a broader privacy policy, which details the general personal information handling processes of the organisation. APP 1 lists the information which is required to be included in a privacy policy.

In practice, a major Privacy Act compliance issue often arises because organizations fail to recognize that the mandatory notice requirements outlined above also apply to any personal information collected from a third party. Organizations must provide individuals with required notice on receipt of personal information from a third party, even though they did not collect personal information directly from the individual. Unlike Europe, Australian privacy law does not distinguish between "data processors" and "data controllers".

Organizations must not use or disclose personal information about an individual unless one or more of the following applies:

- The personal information was collected for that purpose (the primary purpose) or a different (secondary) purpose which is related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organization to use or disclose the information for that secondary purpose.
- The individual consents.
- The information is not sensitive information and disclosure is for direct marketing and it is impracticable to seek the individual’s consent and (among other things) the individual is told that they can opt out of receiving marketing from the organization.
- A "permitted general situation" or "permitted health situation" exists; for example, the entity has reason to suspect that unlawful activity

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;

relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public.
- It is required or authorized by law or on behalf of an enforcement agency.

In the case of use and disclosure for the purpose of direct marketing, organizations are required to ensure that:

- Each direct marketing communication provides a simple means by which the individual can opt out
- The individual has not previously requested to opt out of receiving direct marketing communications

The above direct marketing requirements apply to all forms of direct marketing. Additionally, specific requirements for commercial electronic messaging are outlined in Electronic Marketing.

The Privacy Act affords additional protections when processing involves sensitive information. Organizations are prohibited from collecting sensitive information from an individual unless certain limited requirements are met, including one or more of the following:

- The individual has consented to the collection and the collection of the sensitive information is reasonably necessary for one or more of the entity's functions or activities.
- Collection is required or authorized by law or a court / tribunal order.
- A "permitted general situation" or "permitted health situation" exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public.
- The entity is an enforcement body and the collection is reasonably necessary for that entity's functions or activities.
- The entity is a nonprofit organization and the information relates to the activities of the organization and solely to the members of the organization (or to individuals who have regular contact with the organization relating to its activities).

Organizations must provide individuals with access to their personal information held by the organization upon an individual’s request. Additionally, individuals have a right to correct inaccurate, out-of-date, and irrelevant personal information held by an organization.

- 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

Under certain circumstances, the organization may limit the extent to which it provides an individual with access or correction rights, including in emergency situations, specified business imperatives, and law enforcement or other public interests.

Further, organizations must provide individuals with the option to not identify themselves, or use a pseudonym, when dealing with the organization, unless it is impractical to do so or the organization is required or authorized by law to deal with identified individuals.

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

Unless certain limited exemptions under the Privacy Act apply, personal information may only be disclosed to an organization outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information. The disclosing / transferring entity will generally remain liable for any act (s) done or omissions by that overseas recipient that would, if done by the disclosing organization in Australia, constitute a breach of the APPs. However, this provision will not apply where any of the following apply:

- The organization reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively provides for a level of protection that is at least substantially similar to the Privacy Act, including as to access to mechanisms by the individual to take action to enforce the protections of that law or binding scheme. There can be no reliance on contractual provisions requiring the overseas entity to comply with the APPs to avoid ongoing liability (although the use of appropriate contractual provisions is a step towards ensuring compliance with the 'reasonable steps' requirement).
- The individual consents to the transfer. However, under the Privacy Act the organization must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the

TRANSFER

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:

organization will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs.

- A "permitted general situation" applies.
- The disclosure is required or authorized by law or a court / tribunal order.

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.

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.

SECURITY

An organization must have appropriate security measures in place (i.e. take reasonable steps) to protect any personal information it retains from misuse and loss and from unauthorized access, modification or disclosure. The Information Commissioner has issued detailed guidance on what it considers to be reasonable steps in the context of security of personal information, which we recommend be reviewed and implemented. Depending on the organization, and how and by which government agency it is regulated, as noted above specific requirements or expectations may also exist and with which organizations should be familiar. An organization must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purpose(s) for which it was collected.

SECURITY

Security

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

Entities with obligations to comply with the Privacy Act must comply with the mandatory data breach notification regime under the Privacy Act.

The mandatory data breach notification includes data breaches that relate to:

- Personal information
- Credit reporting information
- Credit eligibility information
- Tax file numbers

In summary, the regime requires organizations to notify the OAIC and affected individuals of "eligible data breaches" (in accordance with the required contents of a notice). Where it is not practicable to notify the affected individuals individually, an organization that has suffered an eligible data breach must make a public statement on

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).

its website containing certain information as required under the Privacy Act, and take reasonable steps to publicise the contents of the statement.

An "eligible data breach" occurs when the following conditions are satisfied in relation to personal information, credit reporting information, credit eligibility information or tax file information:

All of the following conditions are satisfied:

- There is unauthorized access to, or unauthorized disclosure of, or loss of the information;
- A reasonable person would conclude that the access or disclosure, or loss would be likely to result in serious harm to any of the individuals to which the information relates; and
- Prevention of the risk of serious harm through remedial action has not been successful.

While "serious" harm is not defined in the legislation, the OAIC has released guidance on how serious harm may be interpreted and assessed by organizations. There are a number of key criteria to examine when determining if "serious" harm is likely to result from a breach which should be assessed holistically and take into account: the kinds of information, sensitivity, security measures protecting the information, the nature of the harm (i.e. physical, psychological, emotional, financial or reputational harm) and the kind(s) of person(s) who may obtain the information.

The regime also imposes obligations on organizations to assess within 30 calendar days whether an eligible data breach has occurred where the organization suspects (on reasonable grounds) that an eligible data breach has occurred, but that suspicion does not amount to reasonable grounds to believe that an eligible data breach has occurred.

There are various exceptions to the requirement to notify affected individuals and / or the OAIC of a data breach notification including in instances where law enforcement related activities are being carried out or where there is a written declaration by the Information Commissioner.

The introduction of the regime has resulted in many organizations requiring detailed contractual obligations with third party suppliers in relation to cybersecurity and the protection of personal information of their customers / clients. Complimenting this regime, the OAIC has also released several guidance notes relating to the regime

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)).

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.

which include topics such as the security of personal information and whilst these are not legally binding, they are considered industry best practice.

Further, organizations may have additional obligations to notify other regulators of data breaches in certain circumstances including under the Prudential Standard CPS 234 Information Security ("**CPS 234**") which aims to strengthen APRA-regulated entities' resilience against information security incidents (including cyberattacks), and their ability to respond swiftly and effectively in the event of a breach. CPS 234 applies to all APRA-regulated entities who among other things, are required to notify APRA within 72 hours "after becoming aware" of an information security incident and no later than 10 business days after "it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner".

ENFORCEMENT

The Information Commissioner is responsible for the enforcement of the Privacy Act and will investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint about the act or practice has been made. Generally, the Information Commissioner prefers mediated outcomes between the complainant and the relevant organization. Importantly, where the Information Commissioner undertakes an investigation of a complaint which is not settled, it is required to ensure that the results of that investigation are publicly available. Currently, this is undertaken by disclosure through the OAIC website of the entire investigation report.

The Information Commissioner may also investigate any "interferences with the privacy of an individual" (i.e. any breaches of the APPs) on its own initiative (i.e. where no complaint has been made) and the same remedies as below are available. With a number of large scale, high profile data breaches occurring in Australia recently, the Information Commissioner appears to be adopting a more proactive and more publicised approach to investigation and enforcement action, and it seems likely that the review and likely revision of the Privacy Act will strengthen the Information Commissioner's powers with respect to investigation and enforcement.

After investigating a complaint, the Information Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the

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).

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

organization rectify its conduct or that the organization redress any loss or damage suffered by the complainant (which can include non-pecuniary loss such as awards for stress and / or humiliation). The maximum penalties that may be sought by the Information Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals were increased significantly to the greater of (i) AUD50M, (ii) three times the benefit of a contravention, or (iii) (where the benefit cannot be determined) 30% of domestic turnover.

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 sending of electronic marketing (referred to as "commercial electronic messages" in Australia) is regulated under the Spam Act 2003 (*Cth*) (“**Spam Act**”) and enforced by the Australian Communications and Media Authority.

Under the Spam Act, a commercial electronic message (which includes emails and SMS's sent for marketing purposes) must not be sent without the prior opt-in consent of the recipient.

In addition, each electronic message (which the recipient has consented to receive) must identify the sender and contain a functional unsubscribe facility to enable the recipient to opt out of receiving future electronic marketing. Requests to unsubscribe must be processed within 5 business days.

A failure to comply with the Spam Act (including unsubscribing a recipient that uses the unsubscribe facility) may have costly consequences, with repeat offenders facing penalties of up to AU$2.2 million per day.

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 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.

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 are no laws or regulations in Australia specifically relating to online privacy, beyond the application of the Privacy Act, the Spam Act and State and Territory privacy laws relating to online / e-privacy, and other specific laws regarding the collection of location and traffic data. Specifically, the are no specific legal requirements regarding the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organization must comply with the Privacy Act in respect of collection, use, disclosure and storage of such personal information. App developers must also ensure that the collection of customers' personal information complies with the Privacy Act and the Information Commissioner has released detailed guidance on this.

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

Nicholas Boyle
Partner
T +61 2 9286 8479
nicholas.boyle@dlapiper.com

Sarah Birkett
Special Counsel
DLA Piper Australia
T +61 3 9274 5464
sarah.birkett@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.