DATA PROTECTION LAWS OF THE WORLD

Colombia vs Germany

DLA PIPER

COLOMBIA

Last modified 28 January 2024

LAW

Colombia recognizes two fundamental personal data rights under Articles 15 and 20 of its Constitution: (1) the right to privacy and (2) the right to data rectification. Personal data processing is further regulated by two statutory laws and several decrees that set out data protection obligations.

Statutory Law 1266 of 2008 (Law 1266) regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad. Law 1266 defines general terms on habeas data and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data.

Law 1266 defines the terms Data Subject, Data Source, User of Data and Data Operator, as follows:

- ‘Data Subject’ means the owner of the information;
- ‘Data Source’ means a person or entity who receives or collects the information in the context of a commercial relationship with the Data Subject and shares this information with the Data Operator;
- ‘User of Data’ means a person or entity who accesses databases and uses the information gathered by the Data Operator;
- ‘Data Operator’ means a person who manages a database with information provided by the Data Sources and shares it with Users of Data, under the rules provided by Law 1266. The most common example of a Data Operators is a Credit Bureau.

Law 1266 provides the applicable rules and conditions for Data Sources to share information with Data Operators and for such Data Operator to manage and share the information with Users of Data. Notwithstanding this, the Law privileges processing for purposes of managing financial, credit, commercial and services information, considering that this benefits the financial and credit activity as a public interest activity.

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

Law 1266 was amended by Law 2157 of 2021. The main modifications introduced by Law 2157 are the following:

- Data whose content refers to the time of default of an individual or a company, or data that refers to a lack of compliance with monetary obligations, shall be erased immediately or as promptly as possible. This erasure requirement applies mainly to small companies, small farmers, armed conflict victims, young people, women from rural areas, and other debtors who are in special situations, with the specificities foreseen in the Law.
- The obligation to update credit scores was created, provided that any negative data is erased.
- The Law established that the frequent consultation of a person’s credit history should not be a factor for lowering their credit rating.
- Claims and requests concerning the processing of financial data must be resolved within fifteen (15) working days from the date of receipt of the communication. If a prompt resolution is not given within this timeframe, the request is presumed accepted for all legal purposes.
- Financial data, credit records, and commercial information may not be used in making employment decisions.
- The Law introduced the principle of accountability for the processing of financial information. This update implies the Data Source and the Data Operator should adopt internal policies to guarantee the safety and confidentiality of the information.

Furthermore, Statutory Law 1581 of 2012 (Law 1581) regulates all personal data processing, as well as databases. Law 1581 defines special categories of personal data, including sensitive data and data collected from minors. Under the law a ‘Data Controller’ is a legal or natural person responsible for data treatment, or processing, and a ‘Data Processor’ is a legal or natural person in charge of personal data processing. The Data Controller creates databases on its own or in association with others, while the Data Processor processes personal data on behalf of the Data Controller. Nevertheless, an entity may be regarded as both Controller and Processor of personal data.

The law further regulates the obtention of authorization to treat personal data and the procedures for data processing. Moreover, the law creates the National Register of Data Bases (NRDB).

especially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data

Law 1581 is applicable to all data collection and processing in Colombia, except data regulated under Law 1266 and certain other types of data or regulated industries. The law is further applicable in any case where a data processor or controller is required to apply Colombian law under international treaties.

Law 1581 does not regulate:

- Databases regulated under Law 1266;
- Personal or domestic databases;
- Databases aimed to protect and guarantee national security, prevent money laundering and terrorism financing;
- Intelligence and counter-intelligence agency databases;
- Databases with journalistic information and editorial content; and
- Databases regulated under Law 79 of 1993 (on population census).

Law 1581 further requires Data Controllers and Data Processors to guarantee that personal data: is maintained pursuant to strict security measures and confidentiality standards, will not be modified or disclosed without the data subject’s consent, and will only be used for purposes identified in a privacy policy or notice.

Decree 1377 of 2013 (Decree 1377), is a piece of secondary regulation related to Law 1581 which outlines requirements for personal and domestic databases regarding authorization of personal data usage and recollection, limitations to data processing, cross-border transfer of data bases and privacy warnings, among others. This Decree also requires controllers and processors to adopt a privacy policy and privacy notice.

Decree 886 of 2014 (Decree 886) and Decree 090 of 2018 (Decree 090) issued by the Ministry of Commerce, Industry and Tourism, regulate the National Register of Data Bases and sets deadlines for registration of existing data bases in Colombia.

Lastly, Title V of the Sole Circular issued by the Superintendence of Industry and Commerce provides additional guidelines regarding the following matters: (i) the processing of financial data, credit records and commercial information; (ii) the National Register of Data Bases and (iii) International Data Transfers.

DEFINITIONS

The Colombian data protection regime distinguishes between personal data and a sub-category of sensitive

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

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low

personal data, depending on the information and the harmful effects caused by its unlawful use. Law 1266 and Law 1581 contain particular rules related to sensitive personal data.

Definition of personal data

Under Law 1266, personal data is defined as any information related to or that may be associated with one or several determined or determinable natural or legal persons. Personal data may also be regarded as public, private or semi-private data. Public data is available to the public based on a legal or constitutional mandate. Private or semi-private data is data that does not have a public purpose, is intimate in nature and the disclosure of which concerns only the data subject.

Under Law 1581, personal data is defined as any information related to, or that may be related to, one or several determined or determinable individuals, meaning natural persons only.

Definition of sensitive personal data

Under Law 1266, sensitive personal data is defined as data that due to its sensitivity is only relevant to its owner.

Under Law 1581, sensitive personal data is any data that affects its owner’s intimacy or whose improper use might cause discrimination. Data that reveals any of the below information is considered sensitive data and its processing is prohibited by law:

- Ethnic or racial origin
- Political orientation
- Religious or philosophic convictions
- Membership in labor unions, human right groups or social organizations
- Membership in any group that promotes any political interest or that promotes the rights of opposition parties
- Information regarding health and sexual life, and
- Biometrics

Sensitive personal data shall only be processed:

- With the Data Subject's special and specific consent
- If necessary to preserve the data subject’s life, or a vital interest and the Data Subject is physically or legally unable to provide consent
- If used for a legitimate activity and with all necessary security measures, by an NGO, an association or any kind of nonprofit entity, in

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

which case, the entity will need the Data Subject's consent to provide the sensitve personal data to third parties
- If such data is related to or fundamental to exercising a right in the context of a trial or any judicial procedure, or
- If such data has a historic, statistical or scientific purpose, in which case the Data Subject's identity may not be disclosed

NATIONAL DATA PROTECTION AUTHORITY

According to Law 1266, there are two different authorities on data protection and data privacy matters.

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 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

The first of them, which acts as a general authority, is the Superintendent of Industry and Commerce (SIC). The second authority is the Superintendence of Finance (SOF), which acts as a supervisor of financial institutions, credit bureaus and other entities that manage financial data or credit records and verifies the enforcement of Law 1266.

Nevertheless, under Law 1581, the SIC is the highest authority regarding personal data protection and data privacy. It is empowered to investigate and impose penalties on companies for the inappropriate collection, storage, usage, transfer and elimination of personal data.

(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

Law 1581 created the National Register of Data Bases (NRDB). Databases that store personal data and whose automated or manual processing is carried out by a natural or legal person, whether public or private in nature, in the Colombian territory or abroad, shall be registered in the NRDB. Database registration is also required if Colombian law applies to the data controller or data processor under an International Law or Treaty. Registration is mandatory for data controllers that are either of the following:

- Companies or nonprofit entities that have total assets valued above 100,000 Tax Value Units (TVU), meaning COP 3.800.400.000 million (USD 950.100)[1]
- Legal persons of public nature

Decree 866 states that each data controller shall register each one of its databases, independently and must distinguish between manual and automatized databases. In addition, in order to register each database, the data controller or data processor shall provide the following information:

- Identification information of the data controller, such as: business name, tax identification number, location and contact information
- Identification details of the data processor, such as: business name, tax identification number, location and contact information
- Contact channels to grant data subjects rights
- Name and purpose of the database
- Form of processing (manual / automatized)
- Security standards
- Privacy policy

All data bases were required to register by January 31,

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.

2019. Any new data base(s) shall be registered within the 2 months following its creation.

Any substantial change to any of the abovementioned items, shall be updated in the National Registry of Data Bases. For this purpose, substantial changes are considered as any changes that are made in regards to the purposes of the databases, the data processors, the channels to process any claim or request from the data subject, the class or type of personal data, the security measures implemented, the data privacy policy and/or the international transfer or transmission of personal data.

Such updates shall be made:

i. Within the 10 first days of the month in which the substantial change was made,

and

ii. Yearly (between January 2 and March 31 of each year).

Moreover, through the National Register of Data Bases, data controllers shall inform of the following:

i. Any claim submitted by a data subject to the data controller and/or data processor, within each semester of the year. This information shall be registered within the first 15 business days of February and August of each year with the information of the previous semester.
ii. Any breaches of registered data bases. Such report shall be submitted within the 15 business days following the day on which the data controller had knowledge of the data breach.

Footnote 1: Based on the Tax Value Unit for 2022 (COP $38.004 (approximately USD 9.5)). The Tax Value Unit is updated yearly by the Colombian tax authority.

DATA PROTECTION OFFICERS

There is no requirement to appoint a formal data protection officer in Colombia. However, companies are required to appoint either a specific person, or a designated group within the company to be in charge of personal data matters, specifically the handeling of Data Subject rights and privacy request .

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

The processing of financial data, credit records and commercial information, collected in Colombia or abroad, does not require authorization from the Data Subject.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of

However, this information may only be disclosed to:

- The Data Subject or authorized third parties, pursuant to the procedure established by law
- The Users of the Data
- Any judicial or jurisdictional authority upon request
- Any control or administrative authority, when an investigation is ongoing
- Data processors, with the Data Subject’s authorization, or when no authorization is needed , and the database aims for the same objective or involves an activity that may cover the purpose of the disclosing data processor

On the contrary, Law 1581, requires the authorization of the Data Subject for the data controller to process private and semi-private personal data. For the authorization to be valid it must be obtained prior to the data processing and must be "informed", meaning that the data subject must have been made aware of the exact purposes for which the data is being processed. Decree 1377 requires the following:

- Personal data shall only be collected and processed in accordance with the purposes authorized by the Data Subject.
- Such authorization may be obtained by any means, provided that it allows subsequent consultation.

Authorization is not required when:

- A public or administrative entity demands the information through a judicial order or exercising its legal duties.
- It is public data.
- A medical or sanitary urgency requires the processing of personal data.
- The data processing is authorized by law for historical, statistical or scientific purposes.
- The data is related to people’s birth certificates.

Regarding sensitive personal data, Section 6 of Decree 1377 states that the data controller shall do the following:

- Expressly inform the Data Subject that he or she is not compelled to provide sensitive personal data
- Expressly identify what data to be collected and processed is sensitive and
- Obtain the Data Subject's express consent prior to the processing of their sensitive personal data

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

In any case, silence is not considered a reasonable means of obtaining authorization for personal data or sensitive personal data processing.

Furthermore, when collecting personal data of children, both the data controller and the data processor shall ensure that personal data processed serves and respects the children’s superior interests and guarantees their fundamental rights. For these purposes, the child's legal representative (parent or guardian) must authorize the processing of their child’s personal data.

Privacy policy and privacy notice

Decree 1377 establishes the obligation for data controllers to develop a privacy policy that governs personal data processing and ensures regulatory compliance. For this reason, privacy policies are mandatory for all data controllers and shall be clearly written; Spanish is recommended. Finally, according to the Decree 1377, the minimum requirements for the privacy policy are:

- Name, address, email and phone number of the data controller
- Processes and handling of data and the purpose of such processing
- Rights of the Data Subject
- Individual or department within the data controller that is responsible for the attention to requests, consultations and claims to update, rectify or suppress data and to revoke authorization
- Procedure to exercise the abovementioned rights, and
- Date of creation and effective date

The privacy notice is a verbal or written communication by the data controller, addressed to the data subject, for processing her/his personal data. In this communication, the data subject is informed about the privacy policies of the data controller, the manner to access them and the purposes of the treatment.

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

Per Law 1581, the transfer of personal data occurs when the data controller or the data processor located in Colombia sends the personal data to a recipient, in Colombia or abroad, who is responsible for the personal data, *ie*, a data controller.

Cross-border data transfers are prohibited unless the country where the data will be transferred to provides at least equivalent data privacy and protection standards and adequate safeguards to those provided by Colombian law. In this regard, adequate levels of data protection will be

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

determined in accordance with the standards set by the SIC.

This restriction does not apply in the following cases:

- If the Data Subject expressly consented to the cross-border transfer of data
- Exchange of medical data
- Bank or stock transfers
- Transfers agreed to under international treaties to which the Colombia is a party
- Transfers necessary for the performance of a contract between the Data Subject and the controller, or for the implementation of pre-contractual measures, provided the data owner consented, and
- Transfers legally required in order to safeguard the public interest

Therefore, the data controller requires the authorization of the Data Subject for transferring the personal data abroad, unless such transfer is to one of the following countries which, according to the SIC, meet the standard of data protection and security levels.

Authorized countries for international transfer of personal data

- Albania
- Argentina
- Austria
- Belgium
- Bulgaria
- Canada
- Costa Rica
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungry
- Iceland
- Ireland
- Italy
- Japan
- Latvia
- Lithuania
- Luxembourg
- Malta

decisions: Andorra, Argentina, Canada (with some

- Mexico
- Netherlands
- New Zealand
- Norway
- Perú
- Poland
- Portugal
- Republic of Korea
- Romania
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United States
- United Kingdom
- Uruguay

The SIC also considers that personal data can be transferred to any country regarding which the European Commission considers to meets its standard for levels of protection.

Transfer of personal data

The transfer of personal data takes place when the data controller provides personal data to a data processor, in Colombia or abroad, in order to allow the data processor to process the personal data on behalf of the data controller. The data subject’s consent is required for the transfer of data, unless an adequate data transfer agreement between the data processor and the data controller is in place.

In this regard, Decree 1377 requires that the aforementioned agreement include the following clauses:

1. The extent and limitations of the data treatment
2. The activities that the data processor will perform on behalf of the data controller, and
3. The obligations the data processor has to data subjects and the data controller

The data processor has three additional obligations when processing personal data:

- Process data according to the legal principles established in Colombian law
- Guarantee the safety and security of the databases
- Maintain strict confidentiality of the personal data

A data controller transferring data to a data processor

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.

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

must identify the data processor in the National Database Register for each database transferred. Finally, the data processor must process the personal data in accordance with the data controller’s privacy policy and the authorization given by the data subject.

SECURITY

Data controllers have the legal duty of guaranteeing that the information under their control is kept under strict security measures. For this reason, data controllers shall ensure that such information will not be manipulated or modified without the Data Subject's consent . For this purpose, the data controller shall develop an information security policy that prevents the unauthorized access, the damage or loss of information, including personal data.

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

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

BREACH NOTIFICATION

In accordance with Chapter 2, Title V of the Sole Circular issued by the SIC, a data breach refers to the violation of security codes or to the loss and unauthorized access of data subjects’ information held in a database managed by data controllers or data processors.

Under section 17. and section 18. of Law 1581, both the data controller and the data processor have a duty to notify the authority (SIC) in case of a breach of security, security risk, or a risk for data administration. Such notification shall be made no later than fifteen (15) business days from the date on which the data breach was detected.

Lastly, the Colombian data protection regime does not provide a threshold for data breach notifications. Hence, if there is a violation to the security codes or a risk in the management of data subjects’ information, data controllers and data processors must notify the breach.

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)).

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

Since privacy and proper maintenance of personal data are fundamental constitutional rights in Colombia, every citizen is entitled to pursue protection before any Colombian judge, via constitutional action. Any judge may order a private or public entity to modify, rectify, secure or delete personal data if it is kept under conditions that violate constitutional rights. Constitutional actions can take up to ten days to be resolved and an order issued and failure to comply may result in imprisonment of the legal representative of the violating entity.

The Criminal Code of Colombia sets out in section 269F that anyone who, without authorization, seeking personal or third party gain, obtains, compiles, subtracts, offers, sells, interchanges, sends, purchases, intercepts, divulges, modifies or employs personal codes or data contained in databases or similar platforms, will be punishable by 48 to 96 months of prison, and a fine of approximately USD 26,700 to USD 267,000.

Finally, since SIC is an administrative and jurisdictional authority, it is allowed to investigate (as mentioned above), request information, initiate actions against private entities, and impose fines up to approximately USD 534,000, and order or obtain temporary or permanent foreclosure of the company, entity or business.

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 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

Law 527 of 1999 (Law 527) regulates e-commerce and electronic marketing, but there is no specific regulation regarding data privacy on electronic marketing. In any case, the Data Subject's consent is required for marketing, whether electronic or not and the processing of any personal data for this purpose shall be in accordance with Law 1581.

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 is no specific regulation regarding online processing of personal data. Thus, online privacy and data processing is governed by Law 1581.

Personal data must not be available online unless there are adequate security measures to ensure that access by any unauthorized user is restricted.

Collection and use of data collected through cookies or similar online tracking tools is prohibited unless the Data Subject has provided consent. Such consent may be obtained by a pop-up informing the user about the company's privacy policy and ways for the Data Subject's to review, manage or disable cookies.

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

Maria Claudia Martinez Beltrán
Partner
DLA Piper Martinez Beltrán
T +57 3174720
mcmartinez@dlapipermb.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.c

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.