DATA PROTECTION LAWS OF THE WORLD

Austria

AUSTRIA

Last modified 27 December 2022

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.

In Austria, the laws concerning the implementation of the GDPR have been adopted gradually. In summer 2017, the existing Data Protection Act 2000 (*Datenschutzgesetz 2000*) was amended by the Data Protection Amendment Act 2018 (*Datenschutz-Anpassungsgesetz 2018*) which constituted the first implementation of various regulations related to GDPR, and was intended to enter into force simultaneously with GDPR. The 'Data Protection Act' (*Datenschutzgesetz, DSG)* has considerably amended the Data Protection Act 2000. In addition to the GDPR, it is now the central piece of legislation in Austria regulating data privacy.

The Privacy Deregulation Act 2018 (*Datenschutz-Deregulierungs-Gesetz 2018*) further amended the DSG. The DSG, as amended by the Privacy Deregulation Act 2018, came into force on May 25, 2018 and is now the applicable regulation in Austria. The DSG also includes the implementation of the Directive (EU) 2016/680.

In addition to the DSG, further amendments to other statutory laws were adopted in order to implement the GDPR (mostly to adapt to the terminology of the GDPR). These amendments were included in the General Data Protection Adjustment Act (*Materien-Datenschutz-Anpassungsgesetz 2018*) and the research-sector specific Data Protection Adjustment Act – Science and Research (*Datenschutz- Anpassungsgesetz 2018 – Wissenschaft und Forschung – WFDSAG 2018*). Further amendments in other laws have been made by the Second General Data Protection

Adjustment Act, which was passed in June 2018 and applies retroactively. Finally, ordinances were also passed regulating respectively the cases where a data privacy impact assessment is obligatory (the Obligatory DPIA Ordinance - *DSFA-V*) and the exemptions from the obligation to conduct a data privacy impact assessment (the DPIA Exemptions Ordinance - DSFA-AV).

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 referred to in Recital 30, with IP addresses, cookies and RFID tags 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 concerns the " **processing**" of personal data. Processing has a broad meaning, and includes any set of operations performed on data, including mere storage, hosting, consultation or deletion.

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 former legislation, 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 DSG does not include any additional definitions or derogations to the GDPR. However, Section 1 DSG, which provides a constitutional (human) right to data privacy, does not use the definition of "data subject" of the GDPR, but rather uses the term "everyone" which is currently interpreted to include legal entities and other organizations too. Consequently, the constitutional (human) right to data privacy, as well as some basic data subject rights, as regulated in Section 1 DSG, also apply to legal entities and other organizations.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is conducted by data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (successor of 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 establishes the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* 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), 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.

The Austrian Data Protection Authority (*Österreichische Datenschutzbehörde*) can be contacted as follows:

Österreichische Datenschutzbehörde
Barichgasse 40-42 1030 Vienna
Austria / Europe
Phone number: +43 1 52 152-0
E-Mail: dsb@dsb.gv.at

If possible, the Austrian Data Protection Authority prefers to communicate via email.

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 (*eg,* 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 organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if one of the following conditions are met:

- 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 data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

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 penalized 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.

The DSG contains in its Section 5 some additional regulation in respect to the rights and obligations of the DPO. Thereunder, the DPO and all persons working for the DPO are obliged to retain confidentiality regarding the identity of the persons that have approached the data protection officer as well as regarding all the circumstances that could reveal the identity of such persons.

Under certain circumstances, the DPO and their assistant personnel have the right to refuse testimony regarding the data obtained in their capacity as data protection officer, if a person employed in a position subject to the data protection officer's supervision is entitled to such right and to the extent that person has exercised such right. All files and other documents of the data protection officer which are subject to this statutory right to remain silent in the aforementioned extent cannot be lawfully seized.

Further regulations in Section 5 concern the DPOs of public organizations.

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 principle of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance, potentially for years after a particular decision regarding processing of personal data. 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 lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

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

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

Special Category Data

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

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce national legislation regarding processing of 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 national legislation (Article 10).

Section 4 Para 3 DSG regulates the processing of data regarding actions punishable under criminal or administrative law, criminal convictions or suspected criminal actions.

Processing must (i) be based on an explicit legal authorization or obligation to process such data or (ii) be justified by a statutory duty of care or legitimate interests pursuant to Article 6 (1) lit f GDPR, and be carried out in a manner ensuring to protect the data subjects interests set out in the GDPR and the DSG.

For example, legitimate interest may be established in recruitment processes for trustworthy personnel.

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, while 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 Europe’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 (*eg,* commonly used file formats recognised 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 (*ie,* 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 Austrian DSG imposes further obligations upon controllers and processors. Pursuant to Section 6, all employees, agents or contractors of a controller or a processor who have access to personal data must be contractually obliged to transfer personal data only after receiving an adequate and documented instruction by their employer (confidentiality

obligation). All employees, agents or contractors of a controller or a processor must be subject to confidentiality undertakings or professional or statutory obligations of confidentiality. Measures must be taken to ensure that all employees, agents or contractors of a controller or a processor are bound by the aforementioned undertakings and/or obligations of confidentiality even after the termination of their respective contract, regardless of the cause or form thereof.

CCTV, or rather more broadly processing of images made in public or private spaces, including related sound recordings, are subject to further regulation and requirements pursuant to Sections 12 and 13 DSG. This provision provides limitations regarding the lawfulness of such processing as compared to Art 6 GDPR, as processing of image data is only permissible in the following cases:

- processing is necessary in order to protect the vital interests of the data subject
- the data subject has given their consent
- the processing is required or permitted by specific statutory law, or
- the interests of the data controller override the interests of the data subjects in the specific case, and the processing is proportionate

Overriding legitimate interests are assumed by the law in some cases listed as examples, such as preventive protection of property or persons on private properties or publicly accessible spaces controller by the data controller.

The capturing of images / CCTV is always prohibited in the following cases:

- processing of images capturing persons in their personal area of life without their express consent
- processing of CCTV images for the purpose of employee monitoring
- the automated comparison of personal data obtained by means of capturing images / CCTV without explicit consent and for the creation of personality profiles with other personal data, or
- the evaluation of personal data obtained by means of image capturing on the basis of special categories of personal data (Art. 9 GDPR) as a selection criterion

In early 2020, the Austrian Data Protection Authority has published a non-binding opinion, referring to two decisions of the Federal Administrative Court, and stating that Sections 12 and 13 DSG are not in line with the GDPR and shall therefore no longer be applied. The Authority shall assess CCTV data processings exclusively on the basis of the GDPR. However, the contents of the Sections 12 and 13 DSG are still practically used as criteria for assessment of the lawfulness of the processing.

Other additional regulations for processing of data include:

- regulation relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Section 7), which allows processing of such data if they are publicly accessible, have been collected lawfully for other research purposes or other lawful purposes, or are pseudonymized; other data may only be processed to the extent there are specific statutory regulations, the data subjects have given their consent or the Data Protection Authority has approved the processing
- further regulation regarding the processing of data for purposes pursuant to Art 89(1) GDPR, most notably for research purposes, included in the Act on Research Organisation (*Forschungsorganisationsgesetz* - FOG); this regulation includes provisions which lessen to some extent the requirements for processing of special categories of data, including in particular the concept of "broad consent", and limit the rights of data subjects in this respect
- regulation relating to the processing of addresses for informing or sending questionnaires to data subjects (Section 8), which in principle requires consent for such processing, but also provides some derogations
- regulation regarding data processing in cases of catastrophes (Section 10)

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 condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules and standard contractual clauses. 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 defense 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.

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

Section 13 DSG imposes further obligations on Controllers in regard to CCTV and / or processing of captured images pursuant to Section 12 DSG. The controller needs to secure the access to the CCTV / captured images in a way that makes any access and / or subsequent alteration of captured images by an unauthorized third party impossible.

BREACH NOTIFICATION

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

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

Where the breach occurs at the level of the processor, they are 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.

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. 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. Under EU case-law regarding competition, 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. It is not yet clear whether this will translate directly to 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 broad 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 provides for specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" because 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. These claims can be made at any competent court.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Furthermore, individuals may lodge a complaint to 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 Austria, the Austrian Data Protection Authority is responsible for the enforcement of the GDPR. Pursuant to Section 11 DSG, the Austrian Data Protection Authority is obliged to impose administrative fines pursuant to the Article 83 GDPR in an adequate way. The Authority should in particular also apply the measures pursuant to Art 58 GDPR in case of first time breaches, in particular the possibility to issue warnings instead of imposing fines.

The fines under the GDPR are imposed under Austrian administrative criminal law. The Austrian administrative criminal law in general does not allow authorities to impose fines against a legal entity, but provides only for the liability of natural persons; in cases where violations are committed by a legal entity, the liable persons are either statutory representatives (directors) or persons appointed as responsible persons for adherence with specific administrative laws. However, the DSG provides a possibility to impose fines against legal entities, in the following cases:

- A violation of GDPR or DSG is committed by a natural person who has power (1) to represent the legal entity or to make decisions on behalf of the legal entity; or (2) has supervisory powers in the legal entity and has committed this offence either alone or as a part of an organ of the legal entity (*eg,* management board)

- An employee of the legal entity violates the provisions of GDPR or DSG and the violation was possible due to insufficient supervision or control by a person by a natural person that has power to (1) represent the legal entity; (2) or to make decisions on the behalf of the legal entity; or (3) has supervisory powers in the legal entity, provided the violation is not subject to criminal law.

The possibility to impose fines against a legal entity or a responsible natural person, as appropriate. If the fine is imposed against a legal entity, the Authority is required to identify a particular natural person whose violations are to be attributed to said entity; the responsible natural person may not be fined for the same breach.

Public bodies cannot be fined for violations of GDPR or DSG.

ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these will involve use of personal data (eg, an email address which includes the recipient's name). The most relevant 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 apply, and marketing consent forms will 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)).

Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State, provides for specific rules on electronic marketing (including circumstances in which consent must be obtained). The ePrivacy Directive is yet to be replaced by a Regulation. However, it is currently uncertain when this is going to happen. In the meantime, 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.

The GDPR or DSG do not specifically address (electronic) marketing, however, the use of personal data for marketing purposes is clearly within their scope. It is arguable that the processing of personal data of the existing customers within the scope of the business is permissible for marketing purposes, and this has become common practice in Austria. For persons who are not yet customers, the consent of the data subjects is generally required.

Electronic marketing is also regulated by the Austrian Telecommunications Act (*Telekommunikationsgesetz* 2021, 'TKG'). Pursuant to the TKG the sending of electronic messages without prior consent of the recipient is unlawful, if the sending is for direct marketing purposes. No consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his or her personal data and the recipient has not previously declared, by requesting to be entered on to the relevant list (maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)), that they do not want to be contacted.

The GDPR implementation Acts do not provide any amendments or derogations in respect of electronic marketing. However, electronic marketing was and still is separately regulated in Austria in the Telecommunications Act *(Telekommunikationsgesetz* 2021, TKG), Section 174, which implements the ePrivacy Directive.

Pursuant to the TKG the sending of electronic messages without prior consent of the recipient is unlawful insofar as the message is sent for direct marketing purposes. Explicit consent is not required where (1) the data have been obtained in

the context of the sale of goods or provision of services; (2) the electronic marketing concerns same or similar goods or services of the sender; (3), the recipient is able to decline easily and with no costs for the use of his or her personal data for electronic marketing, both when the data are collected as well as with each message received ('opt-out'), and the recipient has not previously declared, by requesting to be entered on to the relevant lists (the "Robinson lists", maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) and the Austrian Chamber of Commerce (WKO)), that he or she does not want to be contacted.

ONLINE PRIVACY

Online privacy is specifically regulated by the TKG.

Traffic data

Traffic Data held by communications services providers (CSPs) must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained for purposes of invoicing the services. In such a case, if the invoice has been paid and no appeal has been lodged with the CSP within three months the Traffic Data must be erased or anonymized.

Location data

Location Data may only be processed for emergency services and with consent of the user. Even in case of consent, the user must be able to prohibit the processing by simple means, for free of charge and for a certain time period.

Cookie compliance

The relevant section of the TKG stipulates that a user must give informed consent for the storage of personal data, which includes a cookie. The user has to be aware of the fact that consent for the storage or processing of personal data is given, as well as the details of the data to be stored or processed, and has to agree actively. Therefore obtaining consent via some form of pop-up or click through agreement seems advisable. Consent by way of browser settings, or a pre-selected checkbox etc. is probably not sufficient in this respect.

If for technical reasons the short term storage of content data is necessary, such data must be deleted immediately thereafter.

Online privacy is still specifically regulated by the TKG, and the GDPR implementation acts have introduced only minor amendments thereto. There are no regulations regarding online privacy in the DSG itself.

Media privilege

In an effort to balance freedom of speech and freedom of information publishers as well as owners and employees of media outlets are granted privileges regarding the processing of data for journalistic purposes (Section 9 DSG). Certain Chapters of the GDPR are not applicable to such processings, specifically:

- Chapter II (Principles);
- Chapter III (Rights of the data subject);
- Chapter IV (Controller and Processor);
- Chapter V (Transfers of personal data to third countries or international organizations);
- Chapter VI (Independent supervisory authorities);
- Chapter VII (Cooperation and consistency); and
- Chapter IX (Provisions relating to specific processing situations).

The same exceptions (with the slight difference of Article 5 of Chapter II remaining applicable) are stipulated if data is processed for scientific, artistic or literary purposes.

KEY CONTACTS

Sabine Fehringer
Partner
T +43 1 531 78 1460
sabine.fehringer@dlapiper.com

Stefan Panic
Counsel
T +43 531 78 1034
stefan.panic@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.