Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top-ranked lawyers

Data Protection & Privacy

Austria
Preslmayr Rechtsanwälte

chambers.com

2020

AUSTRIA

Law and Practice

Contributed by:
Christian Kern and Nils Gröschel
Preslmayr Rechtsanwälte see p.14

Contents

1. Basic National Regime

1.1 Laws

The Austrian federal legal system is characterised by a strict hierarchy, with constitutional laws at the highest level, ordinary legislation at the second level and ordinances at the lowest level. However, due to Austria's membership of the EU, even constitutional laws are overruled by EU legislation, for example regulations and directives.

There are multiple constitutional rights regarding privacy in Austria: especially the "right to respect for privacy and family life" in Article 8 of the European Convention on Human Rights (ECHR), which has the status of a constitutional law in Austria, and Article 1 of the Austrian Data Protection Act (*Datenschutzgesetz* – DSG) which also, for historical reasons, has constitutional rank. Article 1 of the DSG grants a fundamental right to data protection to natural persons as well as legal persons.

However, as in all EU member states, the main substantive legal provisions are contained in the General Data Protection Regulation (GDPR), which has direct effect. The DSG, which is, apart from its Article 1, ordinary legislation, provides additional rules concerning data protection. Some of these rules reflect the opening clauses of the GDPR while others are only applicable outside of the scope of the GDPR. There are various further specific data protection rules scattered over many different individual laws. A general right to privacy is also derived from Article 16 of the Austrian Civil Code (*Allgemeines Bürgerliches Gesetzbuch* – ABGB).

In addition, the Austrian Telecommunications Act of 2003 (*Telekommunikationsgesetz* 2003 – TKG) regulates sector-specific data protection for telecommunications and contains, inter alia, special regulations for the use of cookies and the sending of unsolicited messages (so-called spam). These regulations are based on the implementation of the ePrivacy Directive (ePD).

1.2 Regulators

The main regulator with regard to data protection in Austria is the Austrian Data Protection Authority (*Datenschutzbehörde* – DSB)

The DSB acts as the supervisory authority as defined in Article 51 of the GDPR and is competent to perform the tasks set out in Articles 57 and 58 of the GDPR. The DSB primarily monitors compliance with the GDPR and with Austrian data protection laws, punishes offenders and is the main point of contact for data subjects. The DSB is also responsible for imposing fines on natural and legal persons.

DSB investigations and/or proceedings are mostly initiated by reports or complaints. The DSB also investigates or officially starts proceedings on its own if certain facts are brought to its attention. The DSB may demand all necessary clarifications from a controller or processor of a data processing operation under review and request inspection of data processing operations and related documents. For the purpose of the inspection, the DSB, after notification of the owner of the premises and the controller or processor, is entitled to enter premises where data processing is carried out, to put data processing equipment into operation, to carry out the processing operations to be inspected and to make copies of data carriers.

If the operation of a data processing system poses a significant direct threat to the privacy interests of the persons concerned (imminent danger), the DSB may prohibit the continuation of the data processing. Similarly, the DSB may, at the request of a data subject, order a restriction of processing pursuant to Article 18 of the GDPR if the controller fails to comply with a relevant obligation in good time.

Appeals against rulings of the DSB can be made within four weeks to the Austrian Federal Administrative Court (*Bundesverwaltungsgericht*). Within six weeks and under certain circumstances, an appeal against decisions of the Federal Administrative Court may also be lodged with the Austrian Higher Administrative Court (*Verwaltungsgerichtshof*) or a complaint may be filed with the Austrian Constitutional Court (*Verfassungsgerichtshof*).

Because the GDRP provides the option of parallel legal protection, data subjects can also have recourse to civil courts. Decisions of the civil courts may be appealed against at a higher instance. In some cases, the decision of the higher instance may even be contested before the Austrian Supreme Court (*Oberster Gerichtshof*).

The competent authority for violations of the TKG, such as the sending of unsolicited messages, is the Austrian Telecommunications Office (*Fernmeldebüro*) which may impose fines. With a maximum fine of EUR58,000, the range of TKG fines is significantly lower than the range of fines provided for by the GDPR.

1.3 Administration and Enforcement Process

The DSB is bound in its competences by the provisions of constitutional and ordinary law. A decision on a penalty can therefore be imposed only after an investigation and must be sufficiently justified. Fines may be imposed on both natural and legal persons. Imposing fines on authorities and public bodies is not possible in Austria. See also **2.5 Enforcement and Litigation**.

In order to establish the relevant facts, the DSB conducts an official investigation and collects evidence. This may take place in the context of an oral hearing and/or by the submission of documents. The parties are given an opportunity to hear the taking of evidence and to comment on it. This is normally done by means of a written statement. At the end of the procedure, the DSB takes a formal decision on the matter.

The DSB decides on the amount of a fine. The GDPR provides a separate catalogue for the assessment of penalties. This catalogue is based, in particular, on the nature, seriousness and duration of the infringement; the number of persons affected by the processing and the extent of the damage suffered by them. Measures taken to mitigate the damage and full co-operation with the DSB are considered.

Fines can be enforced by way of attachment. Alternatively, a prison sentence, which must not exceed two weeks, is imposed (on natural persons) if the fine proves uncollectable.

1.4 Multilateral and Subnational Issues

As EU legislation, the GDPR supersedes even constitutional laws. Therefore, Austrian law can only be applied to the extent that it is in conformity with EU law, and in particular the GDPR, or to the extent that a subject is outside the scope of EU law. The DSG, which is, apart from its Article 1, ordinary legislation, provides supplementary rules.

1.5 Major NGOs and Self-Regulatory Organisations

A number of Austrian NGOs are active in the field of privacy rights. The biggest is the Austrian Chamber of Labour (*Arbeiterkammer*). The Consumer Information Association (*Verein für Konsumenteninformation*) is a non-profit consumer organisation. Another player is *ARGE Daten* which focuses on the protection of personal data and privacy in the age of global communication. While *noyb*, founded by Max Schrems and others, concentrates on enforcing the existing data protection laws throughout Europe.

Article 80 of the GDPR states that data subjects have the right to instruct non-profit organisations – whose statutory objectives are in the public interest and which operate in the field of protection of the rights and freedoms of data subjects with regard to the protection of their personal data – to lodge complaints on their behalf, to seek judicial remedies and to claim damages. The opening clause of the GDPR, which would enable such organisations to exercise these rights independently, was not explicitly implemented in Austria.

1.6 System Characteristics

The Austrian data protection system follows the EU system but has some specific characteristics. The most prominent and most widely discussed is probably the fundamental right to data protection for legal persons. In the course of the amendment of the DSG on the basis of the GDPR, privacy rights for legal persons should have been eliminated. This failed, however, because the required two-thirds majority in parliament was not reached. Legal persons are therefore still entitled to the confidentiality of personal data concerning them, insofar as there is a legitimate interest in protecting such data. They have a fundamental right to be informed about which of their personal data is being processed and a right to have incorrect data corrected. A further amendment is currently under consideration.

The text of the DSG further stipulates that the DSB will primarily issue warnings rather than impose direct penalties in the event of infringement. It is questionable whether this provision is in line with the GDPR, and the DSB has so far not shied away from directly imposing penalties. In general, the enforcement practice of the DSB is rather lenient and fines are infrequent. The DSB is also understaffed, with approximately 100 unsettled proceedings per staff member. Hence, proceedings initiated through official channels are rare. But when a complaint is filed, the DSB is known to act quickly and thoroughly.

1.7 Key Developments

There were no special developments in data protection and privacy in Austria in 2019.

The greatest public attention was attracted by the imposition of a fine of EUR18 million by the DSB on the Austrian Postal Service (see **2.5 Enforcement and Litigation**).

On an EU level the European Data Protection Board (EDPB) has issued further publications, to which, even if not strictly binding, the DSB mostly adheres, these include:

- Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies;
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) of the GDPR in the context of the provision of online services to data subjects;
- Guidelines 3/2019 on processing of personal data through video devices;
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default;
- Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1); and
- Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing opera-

tions subject to the requirement of a data protection impact assessment

1.8 Significant Pending Changes, Hot Topics and Issues

The most interesting issues for the near future are certainly the development of jurisdiction on the GDPR and whether and, if so, where Austrian law contradicts the GDPR.

Another current topic is the ePrivacy Regulation (ePR) which is currently at the draft stage, is expected to be adopted in 2020 or 2021 and will probably come into force two years later. According to its current (fourth) draft, the ePR will also lead to changes in certain data protection rules, for example with regard to cookies and unsolicited messages. Plans are to adapt the legal conditions, which are currently still based on the ePD, to the stricter system of the GDPR and to introduce similarly high fines.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

As Austrian data protection is mainly based on the GDPR, the rules in Austria are very similar to those in all other EU member states.

Data Protection Officers

Pursuant to Article 37 of the GDPR, a data protection officer must always be appointed when data processing is carried out by a public authority or body, except for courts acting in their judicial capacity; when the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or when the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and personal data relating to criminal convictions and offences. A group of undertakings may appoint a single data protection officer provided that the officer in question is easily accessible from each establishment.

Authorised Collection and Processing

According to the GDPR, the processing of personal data is lawful only if one of the following applies:

- free and informed consent;
- the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Regarding the permissibility of the processing of special categories of personal data see **2.2 Sectoral and Special Issues**.

Privacy by Design or Default

Pursuant to Article 25 of the GDPR, a controller must take appropriate technical and organisational measures, which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirement of the GDPR and protect the rights of data subjects (privacy by design). Controllers must also implement appropriate technical and organisational measures for ensuring that, by default, only the personal data which is necessary for each specific purpose of the processing is processed (privacy by default).

Privacy Impact Analyses

A data protection impact assessment (DPIA) is necessary when the processing of data is likely to result in a high risk of harm to the rights and freedoms of natural persons; in particular in the case of:

- systematic and extensive evaluation of information relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; and
- systematic monitoring of a publicly accessible area on a large scale.

In Austria, a "blacklist" pursuant to Article 35 paragraph 4 of the GDPR (of the kind of processing operations which are subject to the requirement of a DPIA) was adopted in the form of an ordinance (*Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist* – DSFA-V). Contrary to EU and Austrian

law, this ordinance is not actually a list but rather a catalogue of criteria to assess whether or not a certain processing activity triggers the obligation for a data protection impact assessment.

Austria also chose to adopt a "whitelist" pursuant to Article 35 paragraph 5 of the GDPR (of the kind of processing operations for which no data protection impact assessment is required) in the form of an ordinance (*Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung* – DSFA-AV). Unlike the "blacklist", this is actually a list of processing activities.

Privacy Policies
The GDPR stipulates very extensive information obligations towards data subjects (regardless of whether they are external, such as website visitors, or internal, such as employees), which in most cases take the form of a privacy policy which must be made available to the data subject at the time of the initial collection of the data. The privacy policy must identify, among other things, the controller and their contact information. It must specify which data is processed, why it is processed and the legal basis for such processing. When data is passed on to third parties, this must also be made known. Further information obligations apply when data is transferred to third countries or international organisations. The information must, moreover, specify how long the data will be stored. The data subject must also be informed of his or her rights, including the right to appeal to the supervisory authority. Any use of automated decision-making must also be made clear. If a data protection officer has been appointed, his or her contact information must be provided.

Data Subject Access Rights
See **2.2 Sectoral and Special Issues**.

Anonymisation and Pseudonymisation
If data is no longer linked to a person due to complete anonymisation, it is no longer governed by the GDPR or the DSG. Using pseudonymisation, data can be assigned to a data subject only with additional information. The application of pseudonymisation to personal data can therefore reduce the risks run by the data subjects concerned. However, the personal reference is retained, and the data is still subject to the regulations of the GDPR. If feasible, controllers must implement anonymisation or pseudonymisation as measures of data protection by design and default (see above).

Profiling, Automated Decision-Making, Big Data Analysis, and AI
See **5.1 Addressing Current Issues in Law**.

Injury or Harm
Article 82 of the GDPR provides for a very broad concept of damage. It covers physical, material and non-material damage. This also includes, for example, financial losses and reputational damage. Damages awarded must fully compensate the loss incurred. However, punitive damages are not legally permissible in Austria.

2.2 Sectoral and Special Issues

The GDPR breaks down personal data into "normal" personal data and special categories of personal data (formerly "sensitive" data). Such data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of special categories of personal data is only allowed in exceptional cases as listed in Article 9 paragraph 2 of the GDPR.

Pursuant to Article 10 of the GDPR and Article 4 paragraph 3 of the DSG, the processing of personal data relating to acts or omissions punishable by court or administrative authorities, in particular suspicion of the commission of criminal offences, is permitted in compliance with the provisions of the GDPR if there is an explicit legal authorisation or obligation to process such data, if the permissibility of the processing of such data otherwise results from statutory duties of care, or if the processing is necessary to safeguard the legitimate interests of the controller or a third party pursuant to Article 6 paragraph 1 littera f of the GDPR, and the manner in which the data processing is carried out ensures that the interests of the data subject are safeguarded in accordance with the GDPR and the DSG.

Financial Data
Financial data is not categorised as a special category of personal data. Hence, it may be processed in compliance with the general provisions of the GDPR and the DSG. However, the Austrian Banking Act (*Bankwesengesetz*) stipulates the bank's obligation of secrecy according to which banks, their shareholders, board members, employees and other persons working for the bank must not disclose or exploit secrets that have been entrusted or made accessible to them exclusively on the basis of business relations with customers. Other laws governing the financial sector contain similar statutory obligations of confidentiality.

Health Data
Health data is categorised as a special category of personal data and may therefore be processed only in compliance with Article 9 of the GDPR, which also stipulates certain exceptions for the (public) health and social security sectors or emergencies.

Communications Data
Communications data, voice telephony, text messaging or the content of electronic communications are generally not classed as a special category of personal data (except when they contain special categories of personal data). Hence, such information may generally be processed in compliance with the general provisions of the GDPR and the DSG. However, the TKG stipulates strict communication secrecy regarding content data, traffic data and location data. Monitoring, eavesdropping, recording, interception or other surveillance of messages and associated traffic and location data, as well as disclosure of information about them by persons other than a user without the consent of all other users involved is prohibited. The secrecy of correspondence (eg, letters) is stipulated in the Criminal Code (*Strafgesetzbuch*), together with penalties for violations of the communications secret.

Children's Data
Children's or student data is not specially protected by law and not categorised as a special category of personal data. Accordingly, such information may generally be processed in compliance with the general provisions of the GDPR and the DSG. With regard to the conditions applicable to a child's consent pursuant to Article 8 of the GDPR, Austria used the opening clause to provide for the age of fourteen being that from which consent to the processing of data is lawful.

Employment Data
See **2.4 Workplace Privacy**.

CCTV
The GDPR does not provide any regulations regarding video surveillance. Hence, the DSG stipulates in detail when and under which circumstances CCTV is permitted. However, in two recent (not yet legally binding) decisions, the Austrian Federal Administrative Court has reviewed the validity of Sections 12 and 13 of the DSG, which govern CCTV, in the light of the GDPR and stated that for Section 13 and 12 paragraph 4 No 1 DSG there is no opening clause and therefore these provisions are not applicable. Hence, for the time being, the DSB will no longer apply Sections 12 and 13 of the DSG.

CCTV is permitted when:

- it is necessary in the vital interest of a person;
- the data subject has consented to the processing of his or her personal data;
- it is ordered or permitted by special legal provisions; or
- the interests of the controller or of a third party prevail.

Regarding prevailing interests, CCTV is permissible in particular when:

- it serves the preventive protection of persons or property on private land which is used exclusively by the controller and does not extend spatially beyond the property, with the exception of the inclusion of public traffic areas which may be unavoidable for the achievement of the purpose;
- it is necessary for the preventive protection of persons or property in publicly accessible places which are subject to the domestic authority of the controller, due to legal violations which have already occurred or due to a special risk potential inherent in the nature of the place; or
- it pursues a private documentation interest that is not aimed at depicting and identifying uninvolved persons or the targeted registration of objects that are suitable for the indirect identification of such persons.

Recorded personal data must be deleted by the controller once it is no longer needed for the purpose for which it was collected and when there is no other legally stipulated obligation to retain it. Storage for longer than 72 hours must be proportionate and must be separately recorded and justified. The controller must mark any CCTV appropriately.

Internet Issues
All data collected while visiting websites, such as browsing and viewing data, is considered to be personal data when this information can be directly or indirectly allocated to a natural person (or legal person pursuant to the DSG), in particular by reference to an identifier such as a name, an identification number, location data or an online identifier. Such online identifiers can be IP addresses, cookie identifiers or RFID tags.

Hence, all tracking technologies, cookies, beacons, pixels or other technologies which collect data and include such a personal identifier are deemed to process personal data. This processing must only be made under the strict provisions of the GDPR. In particular, the processing must be lawful and data subjects must be informed accordingly. If cookies or other tracking data are used to conduct behavioural advertising, data subjects must be informed of this circumstance as well. The same applies to social media plugins; data subjects must be properly informed of their use.

Consent to the use of all kinds of cookies (and other technologies) for marketing or tracking purposes is mandatory. In case cookies are necessary for the security or functionality of the website (eg, shopping cart function or language settings) it is sufficient to simply inform the data subjects thereof. Accordingly, cookie banners have become the method of choice to obtain consent and provide information.

In two recent decisions, the European Court of Justice (ECJ) has ruled on cases that involve different types of deletion on Face-

book and Google. Google can "only" be obliged to remove certain search results on its European domains, whereas Facebook can be obliged to delete illegal posts (eg, hate speech, terrorist propaganda, abusive material and damage to credit) as well as posts with the same wording and content worldwide. As a "hosting provider", Facebook (as well as the internet forums popular on the websites of daily newspapers, Wikipedia and other social media providers such as Twitter or Instagram) is only responsible for content if it actually has or should have knowledge of illegal content and does not immediately take action to block or delete this information. Hence, at least due to a court order, such information must be deleted or blocked immediately. As the ECJ has ruled, such an obligation can, however, also apply to postings with the same wording or even with the same content, on a worldwide scale. Such a judicial or official deletion order must, however, specify exactly what is meant by "identical in content" and must under no circumstances require an autonomous assessment by the provider. Google, on the other hand, as a search engine does not store any data itself, but only lists links. Therefore, it does not carry the same responsibility as a hosting provider. Only the "right to be forgotten" according to the GDPR is applicable in this case. However, according to the ECJ, this is limited to the area of the member states. This means that Google remains under the obligation to remove objectionable search results in the context of people-searches on its European domains and to take measures to prevent European users from seeing these results on other Google domains.

Data Subject Rights
All data subjects have the right to request, from the controller, access to, and rectification or erasure of, personal data or restriction of processing concerning the data subject; or to object to processing as well as the right to data portability and the right to lodge a complaint with a supervisory authority. Where processing is based on consent, data subjects have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before that withdrawal.

Data subjects must be informed of these rights (as well as other circumstances) at the time data is collected from them, or, when data is not collected directly from them, within one month, or, if the personal data is to be used for communication with the data subject, at the latest at the time of the first communication to that data subject, or, if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed.

Besides the right to erasure, Article 17 of the GDPR also stipulates a special "right to be forgotten": where the controller has made the personal data public and is obliged to erase it, the controller must take reasonable steps, including technical measures, to inform controllers which are processing that personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, that personal data.

Data subjects not only have the right of access to their personal data, but also – where the processing is based on consent or on a contract – to data portability, with regard to which the data subject has the right to receive his or her personal data which he or she has provided to a controller as well as the right to transmit that data to another controller.

Upon exercise of these rights the controller has to provide information to the data subject within one month of receipt of the request. That period may be extended to three months in the case of very complex, or a large number of, requests.

2.3 Online Marketing

The GDPR in general considers (direct) marketing as a legitimate interest on which data processing may be based. As compensation for the general permissibility of data processing for direct marketing purposes, the data subjects are entitled to object at any time without giving reasons to the processing of personal data for such marketing, which includes profiling to the extent that it is related to such direct marketing. Information about this right must be provided at the latest at the time of the first communication with the data subject, must be explicitly brought to the attention of the data subject and must be presented clearly and separately from any other information.

Marketing via e-mail and similar communication techniques requires an opt-in by the recipients. Under the TKG, calls – including sending faxes – for advertising purposes as well as the sending of e-mail, including SMS messages, for the purposes of direct marketing are not permitted without the recipient's prior consent. Prior consent for the sending of electronic mail is not required when:

- the sender has received the contact information for the message in connection with the sale or service to his or her customers;
- this message is for direct marketing of its own similar products or services;
- the recipient has been given the opportunity to refuse such use of the electronic contact information at the time of its collection and, in addition, at each transmission; and
- the recipient has not refused any mailing by being registered on a special do-not-send list.

Behavioural advertising is lawful pursuant to the general provisions of the GDPR. Any automated individual decision-making, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her is not allowed unless the decision is necessary for entering into, or

the performance of, a contract between the data subject and a data controller; this is authorised by law or based on the data subject's explicit consent.

2.4 Workplace Privacy

Employment data is generally not specially protected by law nor categorised as a special category of personal data. Hence, this information may generally be processed in compliance with the general provisions of the GDPR and the DSG. Most data categories regarding the workplace must either be processed for the performance of the employment contract, are necessary for compliance with legal obligations or can be based on the legitimate interests of the employer. Special categories of personal data may only be processed under the strict provisions of Article 9 of the GDPR. According to Austrian case law, consent cannot be obtained lawfully in an employer-employee relationship because it cannot be considered as given freely (except individual consent pursuant to the Austrian Act Adapting Employment Contract Law (*Arbeitsvertragsrechts-Anpassungsgesetz* – AVRAG)).

Pursuant to Article 88 of the GDPR, EU member state law that provides for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context is implemented in the Austrian Labour Constitution Act (*Arbeitsverfassungsgesetz* – ArbVG) and the AVRAG. According to these, the following measures (besides others) require a works agreement in order to be lawful:

The implementation of control measures and technical systems to monitor workers, where such measures (systems) affect human dignity (any implementations going beyond merely "affecting" human dignity – ie, measures which interfere with human dignity – are strictly prohibited anyway). In companies in which no works council has been established the implementation and use of such measures and technical systems is not permitted unless these measures are carried out with the individual consent of each employee.

The implementation of systems for the automated collection, processing and transmission of personal data of employees, which go beyond the collection of general personal data and professional requirements. A works agreement is not required if the actual or intended use of this data does not go beyond the fulfilment of statutory obligations, collective legal regulations or the employment contract. Thus, CCTV, e-learning systems or insider threat detection and prevention programmes would need a works agreement. Where no works council is established the system may be implemented without any further consent as long as it is lawful pursuant to the general provisions of the GDPR.

The implementation of systems for the assessment of employees, insofar as these systems are used to collect data which is not justified by the use of the data in the company, similarly requires a works agreement.

Whistle-blower hotlines and anonymous reporting are generally permissible for as long as the requirements of the ArbVG, if applicable, and the GDPR are met (legal basis, information obligations, etc). Prior to the GDPR, the DSB had developed certain guidelines with regard to the data subjects, categories of data, storage period and other circumstances under which whistle-blowing hotlines were permissible. These guidelines can still be used to assess the general permissibility of such a system.

Employers are free to regulate the use and restrictions with regard to any hardware or software provided to employees. Thus, blocking of certain websites is allowed. In case employees are monitored in some way – eg, by using digital loss prevention technologies or by scanning websites – a works agreement or individual consent is required (see above).

2.5 Enforcement and Litigation

The DSB is the supervisory authority as defined in Article 51 of the GDPR and is authorised to perform the tasks set out in Articles 57 and 58 GDPR. The DSB primarily monitors compliance with the GDPR and Austrian data protection laws, punishes offences and is the main point of contact for data subjects. The DSB is also responsible for imposing fines on natural and legal persons. The proceedings before the DSB are governed by the Austrian General Administrative Procedure Act (*Allgemeines Verwaltungsverfahrensgesetz*) and the Austrian Administrative Penal Code (*Verwaltungsstrafgesetz*).

Pursuant to Article 83 of the GDPR, violation of a GDPR provision is punished by administrative fines of up to EUR20 million or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Affected data subjects may also claim compensation before a civil court in case they have suffered material or non-material damage as a result of an infringement of the GDPR or the DSG.

The leading enforcement case with regard to an administrative fine is the case against the Austrian Postal Service (*Österreichische Post* – Post). The DSB sentenced the Post to pay EUR18 million. The Post had extrapolated the party-political affinity of its customers based on data such as address or age. The main issue to solve is whether that data was actual data that should not have been passed on or whether the disclosure of such projections is or is not problematic. The DSB considered that the Post may collect and process personal data within the scope of its business

as publishers of addresses and direct marketing companies; if, however, the Post creates statistical probabilities about party-political affinity, this is a violation of the GDPR. The Post lodged an appeal; accordingly, the decision is not yet legally effective.

In addition, the Cobin Claims platform (an NGO aiming to help consumers, small businesses and private investors to assert their rights through collection campaigns to organise class actions) has collected around 1,500 complaints. Cobin Claims wants to enforce up to EUR3,000 per case in damages from the Post in a class action. In a first civil procedure the court awarded the plaintiff EUR800 in non-material damages. This ruling is also not final; both the Post and the plaintiff have filed an appeal.

Regarding class actions in general, previous efforts to implement such an instrument in the Austrian legal system have not been successful. If the similar claims of numerous claimants are to be filed in a single action, this must be done by means of an auxiliary construction, which is referred to as an "Austrian-style class action". Its admissibility has meanwhile been recognised by the case law of the Austrian Supreme Court. For the Austrian-style class action, claimants assign their claims against the same defendant to an entity (eg, a specially founded association, a limited liability company or – in consumer matters – to a consumer protection organisation) which collects these claims and asserts them jointly in the same action. In this case, the suit involves only two parties, although a multitude of claims of different parties are concerned. A prerequisite, however, is that the court seized must be competent for each and every claim (exception: claims that fall within the jurisdiction of the District Courts may be filed with the Regional Courts if the action also contains claims for which regional courts are competent). In addition, the same issues of facts or law must apply to all claims, and there must be an essentially similar ground for the claim.

Under the same conditions, it would also be permissible for claimants not to assign their claims to another entity pursuing the claims on their behalf, but to pursue their claims as plaintiffs themselves together with others in one and the same action, which entails an "accumulation of claims" in multi-party proceedings. In practice, "Austrian-style class actions" relating to the same subject-matter are often conducted at the same time at different Austrian courts (for the purpose of risk spreading and/or in order to benefit from favourable decisions by other courts seized in this matter). In this context, it should be noted that there is no binding effect of the decision in one action on another. Nevertheless, the courts involved adhere de facto to decisions issued by other courts, especially to decisions of a higher instance.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Article 2 paragraph 2 littera d of the GDPR excludes from its material scope the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public security. These types of processing are regulated by Directive (EU) 2016/680, which was implemented in the DSG. These regulations therefore take precedence over the other regulations of the DSG and also the regulations of the GDPR.

The DSG includes extensive provisions for processing for these purposes. Among others, data must be collected lawfully and fairly and for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes. There are extensive correction and deletion obligations and extensive data security measures must be taken.

In principle, processing of personal data is only lawful if it is provided for by law, is necessary and proportionate for the performance of a task and is carried out by the competent authority.

According to the Austrian Code of Criminal Procedure (*Strafprozessordnung* – StPO), the Criminal Investigation Department of the police can access data in various ways. For example, they can search computers and data carriers or request communication data and their contents from providers. Also, permanent monitoring of the electronic communication is possible in principle. These actions must normally be ordered by the public prosecutor's office on the basis of a court order. However, in the event of imminent danger, the Criminal Investigation Department is entitled to carry out less severe actions without an order or authorisation.

A legal protection officer must be appointed by law to monitor the respective authority. In the performance of his or her duties, this representative is independent and not bound by any instructions.

3.2 Laws and Standards for Access to Data for National Security Purposes

The Austrian National Police-provided Security Act (*Polizeiliches Staatsschutzgesetz* – PStSG) stipulates that certain data can be accessed and further processed to protect key state interests, such as protecting constitutional institutions, critical infrastructure or the population from terrorism. These tasks are primarily carried out by the Federal Office for the Protection of the Con-

stitution and the Fight against Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* – BVT). This authority can act largely independently of judicial approval, but is subject to control by the Ministry, Parliament and the courts.

Under this law, data may be processed only within the framework of proportionality. In addition, for special categories of personal data, reasonable precautions must be taken to protect the confidentiality interests of the persons concerned.

A legal protection officer must be appointed by law in such cases.

3.3 Invoking a Foreign Government

Under certain circumstances, a request for access from a foreign government may be considered a legitimate interest within the meaning of Article 6 paragraph 1 of the GDPR. However, the individual case and the concrete interests of the person concerned will have to be considered. No CLOUD Act agreement has been concluded with the USA.

The judgment of a court or tribunal, or the decision of an administrative authority of a third country, requiring a controller or processor to transfer or disclose personal data is only recognised or enforceable in any manner when based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the European Union or a member state.

3.4 Key Privacy Issues, Conflicts and Public Debates

State surveillance of Austrian citizens is a recurrent topic in Austria. An example would be data retention which is planned and has already existed in the past. Similarly, ways and means of access by American authorities and secret services to data located in Europe or stored by American services are a constant source of controversy.

4. International Considerations

4.1 Restrictions on International Data Issues

Pursuant to the GDPR, data transfers within the EU/EEA are not restricted but transfers to third party countries are permitted only if certain safeguards are in place (see **4.2 Mechanisms That Apply to International Data Transfers**). Austrian law does not stipulate any further restrictions or provisions in this regard.

4.2 Mechanisms That Apply to International Data Transfers

As a general rule, the transfer of personal data is permitted pursuant to the GDPR as long as an adequate level of data protection, comparable with the level within the EU, is guaranteed or, in the absence of such guarantees, transfer is allowed in the case of certain derogations.

Personal data may be transferred outside the EU/EEA when the European Commission has decided that the third country in question ensures an adequate level of protection. Such adequacy decisions currently exist for the following countries: Andorra, Argentina, the Faroe Islands, Guernsey, the Isle of Man, Israel, Japan, Jersey, Canada, New Zealand, Switzerland, Uruguay and the USA (provided the receiving undertaking is Privacy Shield certified).

In the absence of an adequacy decision a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards can be:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;
- standard data protection clauses adopted by the Commission;
- standard data protection clauses adopted by a supervisory authority and approved by the Commission; or
- an approved code of conduct or certification mechanism, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In the absence of an adequacy decision or of appropriate safeguards, a transfer of personal data to a third country may take place on one, inter alia, of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such a transfer due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

- the transfer is necessary for important reasons of public interest; or
- the transfer is necessary for the establishment, exercise or defence of legal claims.

4.3 Government Notifications and Approvals

If one of the requirements stated in **4.2 Mechanisms That Apply to International Data Transfers** is fulfilled, no notification or approval of the DSB is required.

Where a transfer could not be based on a guarantee as stated above and none of the derogations for a specific situation is applicable, a transfer to a third country may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. The controller must inform the supervisory authority of such a transfer.

4.4 Data Localisation Requirements

Due to the general rule of the GDPR stipulating the free flow of data within the EU/EEA there are no requirements to store data in-country. In case of data storage outside the EU/EEA the above requirements must be met.

4.5 Sharing Technical Details

There is no requirement in Austria to share any software code, algorithms or similar technical details with the government or the DSB. Nevertheless, the DSB may demand all necessary clarifications from a controller or processor of the data under review and request inspection of data processing operations and related documents.

4.6 Limitations and Considerations

See **3.3 Invoking a Foreign Government**.

4.7 "Blocking" Statutes

Austria does not have any blocking statutes – ie, laws intended to hinder application of a law made by a foreign jurisdiction. On an EU level, blocking statutes may be adopted.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

There are no special provisions with regard to big data in Austria; neither does the GDPR address this topic in particular nor did the EDPB or the DSB issue any guidance on this topic. Hence, the general principles, such as data minimisation, purpose and storage limitation and the information obligations, also apply to big data.

Automated decision-making including profiling, on the other hand, is governed by the GDPR. Pursuant to its Article 22, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affecting them. Automated decision-making is permitted if it is necessary for entering into, or the performance of, a contract between the data subject and a data controller, if it is authorised by law or based on the data subject's explicit consent. Where the automated decision-making is based on a contract or on consent, data subjects have the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision. With regard to the controller's information obligations, data subjects must especially be informed if any automated decision-making is conducted, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of that processing for the data subject. This also applies to any profiling conducted using cookies.

There are no special provisions with regard to artificial intelligence (including machine learning) in Austria, and the GDPR does not address this topic in particular. Nor has the EDPB or the DSB issued any guidance on this topic.

There are no special provisions with regard to the Internet of Things (IoT) in Austria, and the GDPR does not address this topic in particular. In its Opinion 8/2014 on Recent Developments on the Internet of Things of 2014 (WP 223), the Article 29 Data Protection Working Party (Art29WP) issued guidance on this topic. Its opinion was not endorsed by the European Data Protection EDPB.

There are no special provisions with regard to autonomous decision-making (including autonomous vehicles) in Austria, and the GDPR does not address this topic in particular. In 2017 the Art29WP issued its opinion 03/2017 (WP 252) on processing personal data in the context of Co-operative Intelligent Transport Systems (C-ITS). This opinion, similarly, was not endorsed by the EDPB.

With regard to facial recognition in Austria the DSG stipulates that it is not permitted to automatically compare personal data obtained by means of image recordings without the data subject's express consent, nor for the creation of personality profiles with other personal data. Hence, facial recognition (which uses biometric data) requires the express consent of the data subject. Generally, the use of biometric data for the purpose of

uniquely identifying a natural person is prohibited unless one of the exceptions under Article 9 of the GDPR applies.

Geolocation data is considered as personal data and therefore the general provisions apply. In the context of employment, the use of GPS systems to monitor employees requires a works agreement or the individual's consent.

There are no special (privacy related) provisions with regard to the use of drones in Austria, and the GDPR does not address this topic in particular. In addition to the Opinion 01/2015 (WP 231) on Privacy and Data Protection Issues relating to the Utilisation of Drones of the Art29WP of 2015, the DSB has issued brief guidance with regard to drones, stating that drones are only relevant in terms of data protection law if they collect personal data. A toy or model aircraft without a camera or other sensors is not subject to data protection law. The most common form of a drone relevant to data protection law is an aircraft with a built-in camera that records images and transmits them by radio to the pilot. According to the DSB the provisions regarding CCTV also apply to drones. Under these rules, video surveillance of other people's public or private property as a rule is not allowed, and there may also be civil injunctive relief, or the data protection authority may impose a fine if the necessary conditions are met.

5.2 "Digital Governance" or Fair Data Practice Review Boards

A Data Protection Council has been established at the Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice (*Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz*). This council opines on issues of fundamental importance for data protection, promotes the consistent further development of data protection and advises the Federal Government on legal policy issues in projects relevant to data protection law. The Data Protection Council:

- may make recommendations to the Federal Government and the Federal Ministers with regard to data protection law;
- may prepare or commission expert opinions;
- is given the opportunity to comment on draft laws of the Federal Ministries insofar as they are relevant to data protection law, as well as on ordinances in the federal enforcement area which concern essential questions of data protection;
- has the right to request information and reports from persons in charge of the public sector to the extent that this is necessary for the assessment of projects with significant effects on data protection in Austria; and
- may publish its observations, concerns and suggestions and bring them to the attention of the persons responsible for the public sector.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

See **2.5 Enforcement and Litigation**.

5.4 Due Diligence

There are no special data protection provisions with regard to due diligence processes in corporate transactions in Austria, and the GDPR does not address this topic in particular. Accordingly, such processes are governed by the general provisions, in particular the principles of data minimisation (eg, disclosure only of contracts of key personnel or of exemplary contracts, not of all employees) and where possible and feasible the use of anonymised documents.

5.5 Public Disclosure

There are no special provisions in Austria which require disclosure of an organisation's cybersecurity risk profile or experience, such as filings required of publicly traded companies. However, according to Article 34 of the GDPR, where a personal data breach must be communicated to data subjects, under certain circumstances that communication can only be possible by way of a public announcement.

5.6 Other Significant Issues

There are no other significant data privacy and protection issues not otherwise addressed in this chapter.

Preslmayr Rechtsanwälte has nine partners, one attorney and seven associates who are experts in business law. Clients, both from Austria and around the world, are primarily large and medium-sized businesses in manufacturing, banking, trade, information technology, advertising, tourism and telecommunications. In the area of Austrian and European data protection and privacy law, Preslmayr Rechtsanwälte regularly advises locally and globally operating companies on issues of legal compliance with Austrian and European law and also assists with the creation of any required documentation, including DPAs, privacy policies and DPIAs, as well as with regard to the enforcement of rights of data subjects and communication with Austrian data protection authorities in general. The firm also has broad experience in all areas of IT and telecommunication law. Clients in these fields are multinational consumer electronic companies, software and social media companies, manufacturers of electrical appliances and medical products, VoD providers and life science companies.

Authors

Christian Kern has been a partner with Preslmayr Rechtsanwälte since 2018, having been an associate since 2014. His special areas of expertise are data protection/privacy law, product safety and product compliance law, contract law, corporate law and civil law. He advises national and multinational companies with regard to all areas of data protection and privacy legislation. Christian holds a Magister iuris from the University of Vienna and is a member of the Vienna Bar Association.

Nils Gröschel joined Preslmayr Rechtsanwälte in 2019 as an associate. He specialises in information law, data protection and privacy law as well as intellectual property law. He is also active in the field of civil law, labour law and social law. Nils studied at the University of Tübingen in Germany and holds a Magister iuris from the University of Vienna. He is a member of the Vienna Bar Association.

Preslmayr Rechtsanwälte

Universitätsring 12
1010 Wien, Austria

Tel: +43 1 533 16 95
Fax: +43 1 535 56 86
Email: office@preslmayr.at
Web: www.preslmayr.at/en