COUNTRY COMPARATIVE GUIDES 2021

The Legal 500
Country Comparative Guides

Austria

DATA PROTECTION & CYBER SECURITY

Contributing firm

GRAF ISOLA Rechtsanwälte GmbH

Mag. Marija Križanac, CIPP/E, CIPM

Partner | m.krizanac@grafisola.at

This country-specific Q&A provides an overview of data protection & cyber security laws and regulations applicable in Austria.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

AUSTRIA
DATA PROTECTION & CYBER SECURITY

1. Please provide an overview of the legal and regulatory framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws)?

The most important legal framework governing privacy in Austria is the "Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" ("**GDPR**"). It took effect on May 25, 2018 and applies to each member state of the European Union ("EU"), including Austria. It is a directly applicable legal framework unifying the data protection law within the EU, i.e. it does not require implementation by the EU member states through national law. However, several GDPR provisions allow EU member states to enact national legislation specifying, restricting, or expanding the scope of some GDPR requirements ("**opening clauses**").

The GDPR applies to the processing of personal data conducted wholly or partly by automated means and to the processing other than by automated means of personal data which (are intended to) form part of a filing system, with some exceptions (e.g. purely personal or household activities do not fall within the scope of the GDPR). The GDPR applies to data processing in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing as such takes place in the EU. Under certain circumstances, the GDPR also has extraterritorial effect, e.g. it applies to controllers or processors without an establishment in the EU if they process personal data of data subjects who are in the EU and this processing relates to offering goods or services to or monitoring the behaviour of such data subjects. It is enforced by the supervisory authorities of the EU member states (in Austria: the Data Protection Authority, in German: "*Datenschutzbehörde*", "**DSB**").

Austria enacted the Data Protection Amendment Act 2018 (in German: "*Datenschutz-Anpassungsgesetz 2018*") and the Data Protection Deregulation Act 2018 (in German: "*Datenschutz-Deregulierungs-Gesetz 2018*"), which amended the Data Protection Act (in German: "*Datenschutzgesetz*", "**DSG**") in order to align Austrian data protection law with the GDPR (and to implement the "Directive (EU) 2016/680 of the European Parliament ans of the Concil on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA").

Austria also enacted laws amending various individual legal provisions dealing with data processing that can be found throughout the Austrian legal system.

There are a few ordinances by the Austrian supervisory authority, the Data Protection Authority (in German: "*Datenschutzbehörde*", "**DSB**") dealing with issues that the GDPR left to the supervisory authorities of the EU member states: the Certification Body Accreditation Ordinance (in German: "*Zertifizierungsstellen-Akkreditierungs-Verordnung*", "**ZeStAkk-V**"), the Surveillance Body Accreditation Ordinance (in German: "*Überwachungsstellenakkreditierungs-Verordnung*", "**ÜstAkk-V**"), the Data Protection Impact Assessment Exemption Ordinance (in German: "*Datenschutz-Folgenabschätzung-Ausnahmenverordnung*", "**DSFA-AV**") and the Ordinance on processing activities for which a data protection impact assessment must be carried out (in German: "*Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist*" "**DSFA-V**").

The "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy

in the electronic communications sector (Directive on privacy and electronic communications)" ("**ePrivacy Directive**") was implemented into Austrian law through the Telecommunications Act 2003 (in German: "*Telekommunikationsgesetz 2003*", "**TKG 2003**"). In the last few years, the EU has been working on replacing the ePrivacy Directive with a directly applicable EU regulation, however it seems that it could still take years before a new ePrivacy Regulation is completed and enters into force.

Other laws which are closely linked to Austrian privacy laws are the Austrian cybersecurity laws, e.g. the Network and Information Systems Security Act (in German: "*Netz- und Informationssystemsicherheitsgesetz*", "**NISG**"), the Network and Information System Security Ordinance (in German: "*Netz- und Informationssystemsicherheitsverordnung*", "**NISV**") and the Ordinance defining the requirements and special criteria for qualified entities under the NISG (in German: "*Verordnung über qualifizierte Stellen*", "**QuaSteV**"

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

In Austria **no registration or licensing** is required under the abovementioned laws for processing personal data (however, they may in some circumstances be required under other, not privacy-related laws, such as the Austrian Trade Regulation).

Before the GDPR became applicable, Austria had a "Data Processing Register" – controllers were required to register (and sometimes even get prior approval for) their data processing activities; only a few standardized processing activities were exempted. Under the GDPR, Austria has switched to system of self-responsibility with consultation obligations in individual cases:

- There is no longer an official authority-led register; controllers (and processors) must maintain a so-called "record of processing activities" instead (there is a – practically irrelevant – exemption for controllers/processors with fewer than 250 employees).
- There is no longer an authorisation process; instead the controller has to (i) self-assess the lawfulness of his or her processing activities, e.g. through carrying out a "data protection impact assessment" ("**DPIA**", this is a process required for potentially risky processing activities where the controller determines the inherent risks and draws up procedures / implements measures to meet those risks) and (ii) consult the DSB prior to starting processing activities where the conducted DPIA indicates that – even despite the controller's undertaken efforts – would result in a high risk for the affected data subjects. The DSB has published a "whitelist" with processing activities that do not require a DPIA (and, as a logic consequence, also do not require prior consultation of the DSB) and a "blacklist" with a list of criteria that indicate when a DPIA is required (*see question* 1).

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The terms used in the GDPR are "personal data" (for "regular" data) and "special categories of personal data" (for data of a sensitive nature).

Personal data is defined as any information relating to an identified or identifiable natural person ("**data subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data used 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 GDPR also contains definitions for certain types of special categories of personal data, e.g. **genetic data** ("personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question") **biometric data** ("personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data") and **data concerning**

health ("personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status").

Other "key definitions" can be found in Article 4 GDPR, e.g.

- Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Controller**: natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Processor**: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

4. What are the principles related to, the general processing of personal data or PII?

The GDPR sets out the following principles for the processing of personal data:

- **Lawfulness, fairness, and transparency**: Controllers must process personal data lawfully, fairly, and in a transparent manner in relation to the data subject. This means that every processing activity must be based on one of the legal grounds the GDPR prescribes; the GDPR lists e.g. the consent of the data subject, a legal obligation to process the data, or the pursuit of legitimate interests. Furthermore, information about the processing has to be provided to the data subjects and a transparent communication has to be maintained (especially when dealing with data subject requests/rights) in order to enable them to understand what is happening with their data. The processing also has to be conducted within the reasonable expectations of the data subject.
- **Purpose limitation**: Personal data may only be collected for specified, explicit, and legitimate purposes; and may not be further processed for an incompatible purpose (further processing for compatible purposes is permissible under certain circumstances).
- **Data minimization**: The processing has to be strictly limited to what is necessary and relevant for the pursued purpose.
- **Accuracy**: Personal data must be accurate and up to date; every reasonable step has to be taken to erase or rectify inaccurate data without delay.
- **Storage limitation**: Personal data may not be stored in a form that permits identification of data subjects for longer than is necessary for the purposes of their processing (with a few exceptions).
- **Integrity and confidentiality**: Personal data must be processed in a manner that ensures appropriate security, using appropriate technical and organizational measures to protect in particular against unauthorized or unlawful processing, accidental loss, destruction or damage.
- **Accountability**: Controllers must be able to demonstrate compliance with all of the abovementioned principles.

The individual obligations imposed on controllers and processors build on these principles.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?

Under the GDPR, consent of the data subject is one of the possible and equivalent legal grounds for processing personal data. Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

When controllers use pre-formulated written consent declarations, these must be written in clear and plain language, presented in an intelligible and easily accessible form and – where the consent is embedded in a text dealing with other matters as well – clearly

distinguishable from those other matters. The data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Also, the data subject should be informed of his or her right to withdraw the consent at any time.

There are a few circumstances under which the consent – if used as the legal ground for the data processing – has to be given explicitly (whereas otherwise implicit consent suffices), e.g. the processing of special categories of personal data. Under the DSG, controllers are required to obtain data subjects' explicit consent before an "image processing" (e.g. taking a picture, making a video) in the data subject's highly personal sphere, otherwise the processing is inadmissible. Also, the automated comparison of personal data obtained by means of "image processing" is not permitted without explicit consent of the data subject (as regards the rules on "image processing, *see question 8*).

The GDPR permits member state law to prohibit the use of explicit data subject consent as a legal basis for processing special categories of personal data, however, Austria did not make use of this possibility.

There are situations where consent usually is not a valid legal ground for data processing, especially where there is a clear imbalance between the data subject and the controller because of which it is unlikely that consent was freely given. This is why consent is often not a recommended legal ground for data processing in the employment context – even though

it is not generally excluded that an employer could possibly base his or her data processing on employee consent, there is often a remaining risk of the employee consent being invalid.

In Austria, it is also commonly understood that public bodies cannot base their data processing on consent but rather need a legal/statutory basis (e.g. a legal provision under national law allowing or even requiring data processing) – not because of the imbalance issue described above but because of the Austrian constitutional principle that all state administration/action may be exercised only on the basis of laws.

Under the TKG 2003, communication services operators and information society service providers are prohibited from collecting personal data relating to subscribers/users (this also applies to the usage of cookies and equivalent devices) without their consent unless

- the technical storage or access to such personal data has the sole purpose of transmitting a message over a communications network, or
- the technical storage or access to such personal data is necessary to provide services the subscriber or user expressly requested.

Further, consent is required for so-called "unsolicited communication" (e.g. newsletters, electronic marketing, etc.). There is an exemption where consent for unsolicited communication with the controller's own customers is not required if certain preconditions are met (*see question 18*).

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

The term used in the GDPR is "special categories of personal data" (*see question 3*).

Processing of special categories of personal data is prohibited, unless one of the legal grounds laid down in the GDPR applies, e.g.

- explicit consent of the data subject,
- processing is necessary for carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law,
- processing is necessary for the establishment, exercise or defence of legal claims

The DSG includes a few special provisions regarding the processing special categories of personal data:

- **Processing for archiving, scientific or historical research or statistical purposes**: If special categories of personal data are to be processed, there must be an important public interest in the research and it must be ensured that the personal data are only processed by persons who are subject to a statutory duty of confidentiality with regard to the subject matter of the research or whose reliability in this respect is otherwise credible. In addition, an authorization of the DSB is required.
- **Transmission of personal data in case of a catastrophe**: Special categories of personal data may only be transmitted to close relatives if they can prove their identity and their status as relatives and the

transmission is necessary to protect their rights or those of the data subject.

The GDPR also regulates the processing of **personal data relating to criminal convictions and offences**; this type of data can only be processed when

- Carried out under the control of official authority (e.g. the police) and
- EU or EU member state law authorizes the processing and provides for appropriate safeguards for data subjects' rights and freedoms.

The DSG permits processing personal data relating to acts or omissions punishable by courts or administrative authorities, including suspected criminal offenses and convictions, if the processing is GDPR-compliant and the processing is either based on:

- an express legal authorization or obligation to process such data;
- a statutory duty of diligence; or a necessity for the pursuit of legitimate interests of the controller or a third party, provided the manner in which the data is processed ensures that the interests of the data subject are safeguarded in accordance with the GDPR and the DSG.

7. How do the laws in your jurisdiction address children's personal data or PII?

The GDPR contains a special provision regarding children' s consent in relation to so-called "information society services". If an online service provider offers his or her services directly to a child and uses consent as the legal basis for the processing of the child's personal data, the child has to be at least 16 years old for the consent to be valid. Below this age the consent has to be given or authorised by the holder of parental responsibility over the child. The GDPR allows the EU member states to lower the age of child consent below 16 years old, provided the age is not lower than 13. Austria made use of this possibility and **lowered the minimum age to 14 years** in the DSG. Besides lowering the minimum age, the DSG does not change the requirements for obtaining valid consent from children or impose any additional requirements or restrictions on processing personal data about children. (*For the general consent requirements, see question 5*.)

8. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The DSG contains a few special provisions for certain types of data processing, however they are for the most part not derogations but rather supplemental provisions (e.g. providing addresses for notifying data subjects of and conducting surveys; processing personal data during a catastrophe).

The DSG regulates so-called "image processing" (taking photo/videos, CCTV, etc.) – these provisions include derogations from the general provisions in the GDPR, even though the GDPR does not give the EU member states any room to do so. This is why the Austrian

Federal Administrative Court has questioned these provisions' validity under the GDPR in two decisions. These decisions led the DSB to state in an official newsletter that it will generally no longer apply these provisions and instead determine the lawfulness of image processing solely on the basis of Articles 5 and 6 GDPR. Nevertheless, they are still technically in force.

The DSG varies the data subjects' access right and the right for rectification/erasure. Under the DSG, data subjects' access right do not apply if

- providing the information to the data subject would jeopardize the fulfillment of legally assigned tasks of a controller exercising his or her powers as a public authority or
- complying with the access request would endanger trade or business secrets.

The DSG temporarily limits the obligation to rectify or erase personal data when the controller uses automated data processing and can only carry out the rectification or erasure at certain times because of economic or technical reasons.

9. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

The GDPR imposes the concepts of data protection by design and by default. Not only can they be derived from the general principles (*see question 4*), they are also set forth in Article 25 GDPR.

Data protection by design means that the controller must start taking data protection into consideration as

early as the planning/design phase of his or her processing activities, i.e. before he or she even starts processing personal data, by implementing technical and organizational measures. The controller is free in his or her decision how he or she wants to implement this concept, as long as the measures are appropriate, considering factors such as the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the inherent risks (including likelihood of occurrence and severity). The GDPR mentions a few examples of measures the controller could take, e.g. pseudonymising personal data as soon as possible, enabling the data subject to monitor the data processing, etc.

Data protection by default means that the existing setting options of a data processing system must be preset in such a way that only those data are processed which are necessary for the respective purpose of the processing; i.e no active behavior on the part of the data subjects should be necessary in order to achieve a state that is as data protection-friendly as possible (e.g. no pre-ticked checkboxes). Again, the GDPR does not define any specific measures the controller has to undertake.

The ways controllers meet the requirements of data protection by design and by default are in their nature very controller-specific and processing activity-specific. The European Union

Agency for Cybersecurity (ENISA) has published reports called “Privacy and Data Protection by Design – from policy to engineering” and “Recommendations on shaping technology according to GDPR provisions – Exploring the notion of data protection by default” dealing with practical implementation strategies.

10. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Under the GDPR, controllers (and processors) are obliged to keep so-called “records of processing activities” (*see question 2*). The GDPR defines the **minimum content** of these records of processing activities, e.g. the legal grouds and purposes for the processing, the affected categories of data subjects and personal data, the retention period, descriptions of technical and organizational security measures etc. The records have to be in writing, including in electronic form; they have to be made available to the supervisory authority (in Austria: the DSB) upon request. There is an exemption for organisations employing fewer than 250 persons that is not relevant in practice (because it rarely ever applies due to the preconditions that have to be met).

In practice, organisations use everything from self-made excel-sheet solutions to special third party software to develop and maintain records of processing activities.

Besides maintaining records of processing activities, controllers also have to implement technical and organisational measures enabling them to demonstrate compliance with the GDPR in general. When choosing these measures, the nature, scope, context and purposes of processing as well as the imminent risks (likelihood of manifestation, severity of the consequences) have to be taken into account. This includes inter alia demonstration of the data safety measures taken, of instructions to/education of employees (e.g. written privacy policies), of the conclusion of contracts where necessary (e.g. data processing agreements, joint controllership agreements), of carrying out data protection impact assessments where necessary, etc.

11. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

Controllers are required to consult the competent supervisory authority (in Austria: the DSB) prior to processing where a data protection impact assessment (“DPIA”, this is a process required for potentially risky processing activities where the controller determines the inherent risks and draws up procedures / implements measures to meet those risks) indicates that – even despite the controller’s undertaken efforts – would result in a high risk for the affected data subjects. (*See questions 2 and 12*.)

12. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

Under the GDPR, controllers are obliged to conduct so-called data protection impact assessments (DPIA) regarding processing activities that are likely to result in high risks to data subjects (*see question 2*). The GDPR does not mandate the exact procedure for carrying out such a DPIA, but it lists the following **minimum content**:

- a systematic description of the envisaged processing operations and the purposes of the processing
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes
- an assessment of the risks to the rights and freedoms of affected data subjects
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

In practice, organisations use everything from self-made excel-sheet solutions to special third party software to conduct DPIAs.

Organisations that have appointed a data protection officer ("**DPO**") have to consult the DPO when carrying out the DPIA. The DPIA has to be conducted prior to processing.

The GDPR lists the following scenarios/examples for when a DPIA is required:

- a systematic and extensive evaluation of personal aspects 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; or
- a systematic monitoring of a publicly accessible area on a large scale.

The DSB has published a "whitelist" with processing activities that do not require a DPIA (and, as a logic consequence, also do not require prior consultation of the DSB) and a "blacklist" with a list of criteria that indicate when a DPIA is required.

13. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

The GDPR stipulates an obligation to appoint a data protection officer ("DPO") in the following cases:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- 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,
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

If none of the above applies, no DPO has to be appointed – however, a voluntary appointment is possible. The GDPR allows EU member states to require DPO appointments in additional situations, however, Austria did not make use of this option. The DSG does not change the requirements or obligations applicable to a DPO under the GDPR; it only includes additional provisions specifying these requirements or obligations, e.g.

- The DPO and the persons working for the DPO are bound to secrecy in the performance of their duties. This concerns in particular the identity of data subjects who have approached the DPO and to circumstances that allow for these data subjects to be identified, unless the data subject has expressly released them from their obligation of secrecy. The DPO and the persons working for the DPO may only use the information made available to them for the performance of their duties and are obliged to maintain secrecy even after their duties have ceased.
- If the DPO, in the course of his or her work, obtains knowledge of data for which a person employed by a body that is subject to the control of the DPO has a statutory right to refuse to give evidence, the DPO and the persons working for the DPO are also entitled to this right insofar as this employed person has made use of it. Within the scope of the DPO's right to refuse to give evidence, his files and other documents cannot be seized or confiscated.

The appointed DPO has to be registered with the competent supervisory authority (in Austria: the DSB). A group of undertakings may appoint a single DPO provided that he or she is easily accessible from each establishment.

The DPO has at least the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR or to other EU or member state data protection provisions;
- to monitor compliance with to the GDPR or to other EU or member state data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the DPIA and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 GDPR, and to consult, where appropriate, with regard to any other matter.

14. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).

Controllers are obliged to inform data subjects about their processing activities. The GDPR lays down lists of information that are to be provided to the data subjects (varying slightly depending on whether the personal data was collected directly from the data subject or otherwise), e.g. the identity and contact details of the controller, the details of the processing (e.g. legal basis, purpose of processing, categories of data, retention periods, etc.), data subject rights and so on.

There are no provisions on how this information is to be provided. One of the most common forms used in practice is publishing a data privacy notice on the website and making the data and making the data subjects aware e.g. by including a link in E-mail signatures or in the last step of a web registration process (including a checkbox with which the data subject confirms to having read the data privacy notice). It is important that the **data privacy notice** be easily accessible and written in plain, easy to understand language.

The TKG also contains certain information obligations: Providers of public communications services and providers of an information society service are obliged inform subscriber/users which of their personal data are processed, on what legal basis and for what purposes, and for how long their personal data will be stored, as well as about the possible uses based on the search functions embedded in electronic directories. The information must be given at the start of the legal relationship and in a suitable form, in particular in the context of general terms and conditions.

15. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The obligations laid down in the GDPR are mostly controller-oriented; however, there are some obligations that also apply to the processor, e.g. the obligation to appoint an EU representative pursuant to Article 27 GDPR, the obligation to maintain a record of processing activities pursuant to Article 30 GDPR, the obligation to ensure data security pursuant to Article 32 GDPR, etc. The controller remains fully responsible for the processing activities that he or she outsources to a processor. The controller has to choose a suitable processor with which he or she then has to conclude a data processing agreement that contains at least the **minimum content** laid out in the GDPR for such agreements (*see question 16*), inter alia the following **processor obligations**:

- the obligation to processes the personal data only on documented instructions from the controller and to delete/return them at the end of the provision of the data processing services
- the obligation to ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- the obligation to makes available to the controller all information necessary to demonstrate compliance with the GDPR-prescribed processor obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller
- etc.

16. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?

The controller has to choose a suitable processor which provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. The controller and the processor are obliged to conclude a data processing agreement, the minimum content of which is laid out in the GDPR, e.g.:

- a description of the outsourced data processing (e.g. the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects),
- a number of obligations that the controller has to impose on the processor (*see question 15*).

It is also common practice to lay down specific technical and organisational security measures the processor ought to undertake.

17. Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

Monitoring is not explicitly defined or explicitly regulated in the GDPR (i.e. the "general rules" apply). However, monitoring is mentioned a few times throughout the GDPR (e.g. it can trigger (i) the applicability of the GDPR to controllers and processors not established in the EU, (ii) the obligations to appoint a DPO or (iii) the obligation to conduct a DPIA).

The GDPR defines **profiling** as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. There are special provisions for profiling in the context of so-called "automated individual decision-making". Under the GDPR, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (e.g. automatic refusal of an online credit application or e-recruiting practices without any human intervention). Automated individual decision-making, including profiling, is, however, permissible if it is e.g. necessary for entering into, or performance of, a contract between the data subject and a controller or is based on the data subject's explicit consent.

Even in these cases where automated decision-making is permissible, there are a few **restrictions** that the controller has to comply with: The controller has to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. In general, the controller should also not base his or her automated decision-making on special categories of personal data (with some exceptions).

Under the TKG 2003, communication services operators and information society service providers are prohibited from collecting personal data relating to subscribers/users without their consent unless

- the technical storage or access to such personal data has the sole purpose of transmitting a message over a communications network, or
- the technical storage or access to such personal data is necessary to provide services the subscriber or user expressly requested.

This means that, in general, **cookies and equivalent tracking technologies** require the data subjects' **consent**. There are some uncertainties in Austria on how consent can be validly obtained, especially whether passive behaviour or circumstances such as data subjects' browser settings allowing cookies or continued use of a website with prominent notice regarding the use of cookies can be interpreted as valid consent. The parliamentary guidance on the interpretation of the provisions of the TKG 2003 suggest that this is the case. However, it is doubtful whether this interpretation is compatible with EU law, especially in the light of decisions of the Court of Justice of the European Union ("CJEU", e.g. C-673/17 – Planet49) that indicate a higher standard for valid consent is required. The draft proposals for the ePrivacy Regulation (*see question 1*) suggest that it will follow this trend of a higher standard.

The TKG also contains certain information obligations

(*see question 14*) – the information has to be provided to the data subjects before storing tracking technologies such as cookies on their devices.

18. Please describe any laws in your jurisdiction addressing email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Austria has implemented the "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication)" ("**ePrivacy Directive**")– including its provisions on "unsolicited communication" – in the TKG 2003.

Under the TKG 2003, the sending of electronic mail is not permitted without the prior consent of the recipient if the message is for the purpose of direct marketing ("unsolicited communication). Prior consent for the sending of electronic mail is not required only if

- The recipient is a customer of the sender, i.e. the sender has received the recipient's contact information for the message in connection with the sale of goods or services, and
- The message is for direct marketing of the sender's goods or services similar to those previously acquired by the recipient/customer from the sender and
- the recipient has been clearly and unambiguously given the opportunity to refuse such use of his or her electronic contact information free of charge and without difficulty at the time of its collection and additionally at the time of each transmission (e.g. an unsubscribe-link in a newsletter), and
- the recipient has not rejected receiving direct marketing messages from the outset.

The sending of electronic mail for the purpose of direct marketing is prohibited in any case if

- the identity of the sender is concealed or disguised, or
- the information obligations regarding commercial communication prescribed in the E-Commerce Act are violated, or
- the recipient is requested to visit websites that violate the aforementioned information obligations, or
- there is no authentic address to which the recipient can send a request to stop such messages.

19. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

In the GDPR, biometric data is a type of special categories of personal data (*see question 3*). Biometric data is defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images (facial recognition) or dactyloscopic data (fingerprints).

Biometric data – like all other special categories of personal data – may not be processed unless one of the exemptions provided for in the GDPR applies, e.g. the data subject has given his or her explicit consent. Given that the usage of biometric data is a highly intrusive type of data processing, the controller has to analyse carefully whether the purpose of processing can be fulfilled by other, less intrusive means (e.g. is it really necessary to conduct physical access controls through facial recognition/fingerprint scans etc or would a keycard system suffice?). If this is the case, such less intrusive means have to be chosen instead of the processing of biometric data.

Depending on the circumstances, the intended processing of biometric data might trigger e.g. the obligation to conduct a DPIA (and maybe even to consult the DSB) prior to starting the processing activity and the obligation to appoint a DPA (*please see questions 12 and 13*).

20. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does cross-border transfer of personal data or PII require notification to or authorization form a regulator?)

The transfer of personal data to recipients within the EU/EEA is unrestricted; the transfer to recipients outside the EU/EEA is subject to restrictions. In order for such transfers to be permissible, one of the following cascade-

esque prerequisites has to be fulfilled:

- **Adequacy decision**: A transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country or the international organisation in question ensures an adequate level of protection. A list of countries for which an adequacy decision was issued can be found on the website of the European Commission.
- **Appropriate safeguards**: In the absence of an adequacy decision of the European Commission, a transfer can be based on "appropriate safeguards" listed in the GDPR; e.g. (i) binding corporate rules ("**BCR**") approved by a supervisory authority; and (ii) standard data protection clauses adopted by the European Commission (at the end of 2020 the European Commission published a draft set of such **standard data protection clauses**, however no final versions have been adopted as of the date of this publication; until that happens the old standard contractual clauses issued on the basis of the former Data Protection Directive can still be used).
- **Derogations for specific situations**: In the absence of both an adequacy decision and appropriate safeguards, a transfer can still take place if one of the "specific situations" listed in the GDPR applies (e.g. the data subject has given his or her explicit consent, the transfer is necessary for the performance of a contract with the data subject, the transfer is necessary for the establishment, exercise or defence of legal claims; etc.)
- **One-off transfers**: If none of the above applies, the transfer can still take place if the following prerequisites are met: the transfer is not repetitive, concerns only a limited number of data subjects, 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, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. Also, the controller has to inform the supervisory authority and the data subjects of the transfer.

The GDPR allows EU member states to, for important public interest reasons, enact national laws limiting the cross-border transfer of specific categories of personal data if the destination country has not been deemed to provide an adequate level of data protection. The DSB does not make use of the opening clause.

21. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

Under the GDPR, controllers and processors are obliged to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk inherent to their processing activities. When deciding which measures they should implement (i.e. what is "appropriate" in their individual case), controllers and processors should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Even though the GDPR leaves it open to the controllers and processors to determine and decide which measures to implement, it lists certain measures they should take into consideration, e.g.

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

Also, it obliges controllers and processors to ensure that natural persons acting under their authority who have access to personal data do not process them except on instructions from the controller.

According to the GDPR, adhering to an authority-approved code of conduct or having a certification can also be used "as an element" by which to demonstrate compliance with the abovementioned security obligations.

Unfortunately, in Austria there are still only very few approved codes of conduct; as of the date of this publication the DSB has approved only five:

- code of conduct for internet service providers

- code of conduct for network operators when processing personal data of end users collected with smart meters
- code of conduct for on data protection of the professional association of employers of private educational institutions
- code of conduct for the exercise of the trade of address publishers and direct marketing companies
- code of conduct for the exercise of the accounting profession (accountant, bookkeeper, personnel accountant).

In Austria there are still no approved certification mechanisms available; as of the date of this publication the DSB has not even yet accredited any certification bodies. However, the DSB recently has at least issued an ordinance on the requirements for the accreditation of a certification body.

The TKG 2003 also contains special provisions regarding data safety that apply in parallel to those of the GDPR mentioned above. Pursuant to the TKG 2003, providers of a public communications service are – without prejudice to the provisions of the GDPR – obliged to **ensure the following by means of data security measures in any case**:

- ensuring that only authorized persons have access to personal data for legally permissible purposes;
- protecting stored or transmitted personal data against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage or processing, access or disclosure;
- the implementation of a security concept for the processing of personal data.

The regulatory authority may review the measures taken by the providers of public communications services and make recommendations on the level of security to be achieved. Also, without prejudice to the obligations under the GDPR, in those cases where there is a particular risk of a breach of confidentiality, the provider of a public communications service is obliged to inform subscribers of that risk and, if the risk is outside the scope of the measures to be taken by the provider, of possible remedies, including their costs.

The **NISG** lays down measures designed to achieve a high level of security of network and information systems ("**NIS**") of (i) operators of essential services in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply, digital infrastructure, (ii) digital service providers and (iii) entities of public administration.

Operators of essential services must take appropriate and proportionate technical and organisational security measures to ensure the security of NIS used by them in the context of offering the essential service. Those security measures must have regard to the state of the art and must be appropriate to the reasonably identifiable risk. In its Annex 1, the NISV lists category specific measures that must be implemented, wherever possible, on the basis of a risk analysis. The obligation to take such measures also applies to entities of public administration when offering critical services and to digital service providers in relation to their digital services. The measures relating to digital service providers must consider the security of systems and facilities, security incident handling, business continuity management, monitoring, auditing and testing and compliance with international standards.

Additionally, the NISG provides for notification obligations of security incidents to be fulfilled under certain conditions by operators of essential services, digital service providers or entities of public administration (*see question 24*).

22. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

The term used in the GDPR is "**personal data breach**". A personal data breach is defined as a 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.

In case a personal data breach occurs (and unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons), the controller is obliged to notify the supervisory authority (in Austria: the DSB) without undue delay and, where feasible, **not later than 72 hours** after having become aware of the personal data breach.

The GDPR lays down the following minimum content of such notification:

- Where the notification to the supervisory authority is not made within 72 hours: reasons for the delay A description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- The name and contact details of the data

protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller is obliged to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. He or she is obliged to provide it to the supervisory authority upon request.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is obliged to communicate the personal data breach to the data subject without undue delay. The need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

The communication to the data subject has to describe in clear and plain language the nature of the personal data breach and contain at least the information mentioned in the last three bullet points mentioned above.

Such communication is not necessary, if

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the affected data subjects is no longer likely to materialise;
- it would involve disproportionate effort. (In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.)

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

The DSG does not contain special provisions regarding (the notification of) data breaches (except those implementing the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA). The DSB has provided a form notification that controllers can, but do not have to use to notify a data breach.

The **TKG 2003** also contains provisions regarding security breaches:

In parallel to the GDPR, the TKG 2003 also contains an obligation to notify the DSB (and under some circumstances inform the affected data subjects) without undue delay of a security breach. Providers of public communications services have to maintain a register of personal data breaches. It has to contain information on the circumstances of the breaches, their effects and the remedial measures taken.

Operators of public communications networks or services have to notify the Austrian Regulatory Authority of security breaches or a loss of integrity if this has had a significant impact on network operation or service provision. If disclosure of the breach is in the public interest, the Austrian Regulatory Authority may inform the public itself in an appropriate manner or request the operator

The **NISG** defines “security incident” (in German: “Sicherheitsvorfall”) as any disturbance of the availability, integrity, authenticity or confidentiality of NIS which has resulted in a restriction of continuity or a failure of the service operated with significant impact. The services concerned are essential services, digital services or a critical service provided by an entity of public administration. The service must be unavailable (failure) or qualitatively restricted (restriction) in order to meet the definition. In addition to cyberattacks or third-party interference, a security incident can be caused by physical events such as natural events, as well as events such as power outages or the actions of an agency’s own employees.

When assessing the significance of the impact, particular consideration must be given to the following parameters:

the prospective number of users affected (in particular users relying on the service for the provision of their own services), duration, geographical spread of the interference and the impact on economic and societal activities. For operators of essential services, the parameters for assessing a significant impact are defined in the NISV. As regards digital service providers, the parameters are set out in the Implementing Regulation (EU) 2018/151. In the case of public administration entities, the assessment is at the discretion of the organisation concerned.

Pursuant to the NISG, operators of essential services, digital service providers or entities of public administration must notify, without undue delay, the responsible Computer security incident response teams ("CSIRT") of any security incidents, which forwards the notification to the Federal Minister of the Interior without undue delay. The CSIRT in charge is, where established, the sector-specific CSIRT (currently only set up for the sector of energy), the national CSIRT or the Government Computer Emergency Response Team.

For a digital service provider, the obligation to notify a security incident only applies where the provider has access to the information needed to assess the impact of a security incident. Entities of public administration are only obliged to notify if crucial services provided by them are concerned.

23. Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?

The NISG imposes specific security requirements (i) on operators of essential services in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply, digital infrastructure, (ii) digital service providers and (iii) entities of public administration (*see also question 21*).

24. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

See question 22

25. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

Under Austrian law, there is specific legislation regarding cybercrime incorporated in the Austrian Criminal Code (in German: "Strafgesetzbuch", "**StGB**"). The StGBputs the unlawful access to a computer system under penalty. Essential for the commission of the offense is (i) gaining access by overcoming a specific security measure of the system and (ii) the offender's intention of obtaining knowledge of confidential personal data worthy of protection ("espionage offender") or the intention of inflicting a disadvantage on another person by using data stored in the system or by using the computer system. The penalty increases if the offense is committed in relation to a computer system that is an essential part of the critical infrastructure. Provided the respective conditions are met (in particular, the overcoming of a security measure), ransomware attacks may fall under this provision. In any case, the enforcement of payment of ransoms in ransomware attacks constitutes blackmail by means of dangerous threat under the StGB.

In 2011, the Cybercrime Competence Center ("C4") was established at the Federal Criminal Police Office. As a national and international central office, the C4 is responsible for the electronic preservation and analysis of evidence, investigations in connection with cybercrime in the narrower sense, and the coordination of the fight against cybercrime.

The Ministry of Interior prepares annual reports in order to inform the public about current phenomena and new trends in cybercrime (please access under https://www.bundeskriminalamt.at/306/start.aspx).

26. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

As regards network and information systems security, responsibilities are divided between the Federal Chancellor and the Federal Minister of the Interior. At the Ministry of Interior, a single point of contact ("SPOC") on the security of network and information systems is established. The SPOC exercises a liaison function to ensure cross-border cooperation with the competent bodies in other Member States of the EU and with the Cooperation Group and the CSIRTs network. In addition, the SPOC forwards incoming notifications and requests directly to the members of the ICOCS and the CSIRTs, and informs, upon request, the single points of contact in

other Member States in cross-border matters.

Coordination structures are established, i.e. the Inner Circle of the Operational Coordination Structure – "ICOCS" (an inter-ministerial structure for coordination composed of representatives of specific Ministries) and the "Operational Coordination Structure – "OCS)" (a structure for coordination at the operational level, composed of the ICOCS and the Computer security incident response teams ("CSIRTs")).

On EU level, ENISA (EU's agency for cybersecurity) is established which provides recommendations on cybersecurity, supports development and implementation of policies and collaborates with operational teams throughout Europe.

27. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

The GDPR provides the data subject with the following rights:

- **The right to information**: See question 14.
- **The right of access**: The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and certain information (e.g. the purpose of the processing, the legal ground for the processing, the categories of data being processed, etc.) The controller has to provide a copy of the personal data undergoing processing. Under the DSG, data subjects' access right do not apply if (i) providing the information to the data subject would jeopardize the fulfillment of legally assigned tasks of a controller exercising his or her powers as a public authority or (ii) complying with the access request would endanger trade or business secrets.
- **The right to rectification**: The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- **The right to erasure**: The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds for erasure laid out in the GDPR applies (e.g. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed). The GDPR stipulates a few exemptions where the right to erasure does not apply (e.g. when the data is required for the establishment, exercise or defence of legal claims). The DSG temporarily limits the obligation to rectify or erase personal data when the controller uses automated data processing and can only carry out the rectification or erasure at certain times because of economic or technical reasons.
- **The right to restriction of processing**: The data subject has the right to demand the processing of his or her data to be restricted under certain circumstances (e.g. when the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data). Where processing has been restricted, personal data can only be processed under certain circumstances (e.g. with the data subject's consent or for the establishment, exercise or defence of legal claims).
- **The right to data portability**: The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where a) the processing is based on consent or on a contract and the processing is carried out by automated means.
- **The right to object**: The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on certain legal grounds (public interest, legitimate interest). The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights

and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

- **The rights in relation to automated decision making and profiling**: The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This right does not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent.

Data subjects can exercise these rights by contacting the controller (or the processor, which has to forward the request to the controller). The controller has to respond to data subject requests without undue delay, at the latest within one month (or give reasons where he or she does not intend to comply with such requests or inform the data subject that he or she needs more time – in this case the response time can be extended by two months).

28. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

The GDPR gives the data subject both a right to an effective judicial as well as administrative remedy. It is up to the data subject whether he or she lodges a complaint with the DSB or files a lawsuit with the civil court.

29. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

See question 28. The data subject can file a lawsuit with the civil court if he or she is of the opinion that his or her rights have been infringed.

30. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Pursuant to the GDPR, any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive full and effective compensation from the controller or the processor for the damage suffered. A respective provision is also included in the DSG. A data subject could therefore also potentially demand compensation for non-material damages such as injuries of feelings.

However, proof of an actual injury of feelings could become a stumbling stone in the process of obtaining compensation. The Austrian Supreme Court clarified that the data subject has the burden of proving the damage and causality; the reversal of the burden of proof at the expense of the controller or processor that is stipulated in the GDPR only relates to culpability (they "only" have to prove that they are not in any way responsible for the event giving rise to the damage).

31. How are the laws governing privacy and data protection enforced?

With the aim to ensure consistent monitoring and enforcement of the GDPR throughout the EU, it was decided to give all supervisory authorities in the Member States the same tasks and effective powers. Thus, a list of these tasks and effective powers was added to the GDPR, containing inter alia:

- **Investigative powers** such as the power to carry out investigations in the form of data protection audits, the power to obtain access to all personal data and to all information necessary for the performance of its tasks, the power to obtain access to any premises of the controller and the processor, including to any data processing equipment and means;
- **Corrective powers** such as the power to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR, the power to order the controller or processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified

manner and within a specified period, the power to impose a temporary or definitive limitation including a ban on processing,
- **Authorisation and advisory powers** such as the power to advise the controller in accordance with the prior consultation procedure referred to in Article 36 GDPR, the power to adopt standard data protection clauses, the power to approve binding corporate rules.

With regard to the DSB's power to impose administrative fines, please see question 32.

The DSG contains provisions further specifying some of these powers in order to assure appropriate safeguards and due process as stipulated in the GDPR, e.g. the provision that information obtained by the DSB or its agents in the course of their inspection activities may only be used for inspection purposes within the framework of the enforcement of data protection regulations and that their obligation to maintain confidentiality also applies to courts and administrative authorities, in particular tax authorities (with certain exemptions).

32. What is the range of fines and penalties for violation of these laws?

Depending on the violation, administrative fines under the GDPR range from up to EUR 10 million to up to EUR 20 million, or in the case of an undertaking, up to 2% or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, the supervisory authority (in Austria: the DSB) has to consider a list of factors laid out in the GDPR, e.g.: the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the damage suffered by data subjects, etc.

The **DSG** lists administrative offenses that do not fall under the penalty catalogue of the GDPR which are punishable by fines of up to EUR 50,000, e.g.:

- Intentionally and illegally gaining access to data processing or maintaining an obviously illegal means of access.
- Intentionally transmitting data in violation of the confidentiality provision of the DSG.
- Intentionally obtaining personal data in cases of catastrophe under false pretences.
- Conducting so-called "image processing" in violation of the respective DSG provisions.
- Refusing inspection by the DSB.

Under the **DSG**, anyone who, with the intention of unlawfully enriching himself or a third party or with the intention of damaging another person's right to data protection, uses, makes available to another person or publishes personal data which has been entrusted to him or has become accessible to him exclusively on the basis of his professional employment or which he has obtained unlawfully, even though the person concerned has a legitimate interest in keeping this data secret, shall be punished by the court with a prison sentence of up to one year or a fine of up to 720 daily rates.

The GDPR enables EU member states to specify whether and to what extent supervisory authorities may impose administrative fines on public authorities and bodies. Austria decided to regulate in the DSG that no administrative fines may be imposed on public authorities and public bodies.

The **StGB** also contains provisions that might also apply in cases of data protection infringement; e.g. it sanctions illegal access to a computer system, abusive tapping of electronic data, and manipulation of electronic processing with the intention of unjustified enrichment with a fine or up to six months' imprisonment.

33. Can personal data or PII owners/controller appeal to the courts against orders of the regulators?

A controller can appeal a decision of the DSB before the **Federal Administrative Court** (in German: "Bundesverwaltungsgericht"); the decision of this court can be appealed before the **Supreme Administrative Court** (in German: "Verwaltungsgerichtshof") and – depending on the circumstances of the case – before the **Supreme Constitutional Court** (in German: "Verfassungsgerichtshof").

Contributors

Mag. Marija Križanac, CIPP/E, CIPM
Partner
m.krizanac@grafisola.at