GEISTWERT
RECHTSANWÄLTE LAWYERS AVVOCATI

tel +43 1 585 03 03-0
fax +43 1 585 03 03-99
Linke Wienzeile 4
1060 Wien · Vienna · Austria
www.geistwert.at

Juliane Messner / Max W. Mosing
juliane.messner@geistwert.at / max.mosing@geistwert.at
GEISTWERT Rechtsanwälte, Linke Wienzeile 4, 1060 Vienna, Austria

DATA PROTECTION LAW IN AUSTRIA

Status Case Law: until September 23, 2020

Constitutional Provisions in the Federal Act on the Protection of Personal Data of Natural Persons and Legal Entities

Section 1 of the Austrian Federal Act concerning the Protection of Personal Data (DSG),[1] provides for the fundamental right to data protection in the form of a "constitutional provision." This fundamental right has direct effect on third parties; it creates an obligation, on both the Austrian state and each individual in Austria, to meet the provision (for details see below). Amendments and the name change of the former Austrian Federal Act of 2000 concerning the Protection of Personal Data (DSG 2000) to Austrian Federal Act concerning the Protection of Personal Data (DSG) in the light of the EU General Data Protection Regulation (GDPR)[2] left Section 1 DSG unchanged.

Pursuant to this fundamental right in the form of a constitutional provision, everyone, including natural persons and legal entities (in light of the GDPR, most probably an unique extension of the data protection regime to legal entities), will have the right to secrecy of the personal data concerning the data subject, especially with regard to private and family life, to the extent that the data subject has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy, because they are generally available or because data cannot be traced back to the data subject.[3]

The constitutional provision stipulates that, if personal data is not used in the vital interest of the data subject or with the data subject's consent, restrictions to the right to secrecy are permitted only when necessary to safeguard overriding legitimate interests of another.

In case of an intervention by a public authority, the restrictions are only permitted based on laws necessary for the reasons stated in Article 8, Paragraph 2 of the European Convention on Human Rights.[4] Such laws may provide for the use of data that deserve special protection

[1]Original version in Federal Law Gazette I 1999/165.

[2]EU General Data Protection Regulation, Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation" or "GDPR"), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[3]DSG, Section 1.

[4]Article 8(2) of the European Convention on Human Rights provides: "There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the

only in order to safeguard substantial public interests. They must provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in the case of permitted restrictions, the intervention may be carried out using only the least intrusive of all effective methods.

By statute, with respect to automated and manual data processing, every data subject has the right (1) to information on the data processed with respect to the data subject, including the origin of the data, the intended purpose of the processing, and the recipient(s) and (2) to have inaccurate data corrected and unlawfully processed data deleted.

Even though Section 1 DSG guarantees the fundamental right to data protection for both natural persons and legal entities, the latter can only partially invoke their fundamental right to data protection. As stated in Section 1 DSG, the rights to information, rectification, and erasure require a more detailed non-constitutional legal basis. Such legal basis has not been implemented in Austria.

In accordance with the GDPR, Section 4 DSG even restricts the scope of application of DSG to natural persons. Therefore, there is a gap regarding the procedural regulations enforcing the rights generally provided by the constitutional provision of the DSG (see above). Furthermore, the Austrian Data Protection Authority (ADPA) is not competent to enforce the rights of the legal entities. However, those rights can be enforced with the ordinary (civil and penal) courts in Austria.

European Framework applied in Austria

On May 25, 2018, the EU General Data Protection Regulation, Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) entered into force. Because of its structure as a regulation, rather than a directive, the GDPR became de facto the primary data protection law of each Member State of the EU. Therefore, the GDPR applies also in Austria.

The GDPR provides EU Member States with the ability to modify or supplement the base GDPR with provisions that apply only at the member-state level and that are consistent with the current culture and treatment of personal data in the particular Member State. In addition, the GDPR permits sector-specific data protection laws and regulations in each Member State.

In addition to the GDPR, the relevant national data protection laws of Austria include the following:

- The Austrian Data Protection Act (Datenschutzgesetz, or DSG) supplements the Data Protection Regulation (GDPR). The DSG was extensively modified. The name of the older version of the law was “Datenschutzgesetz 2000" (DSG 2000).
- When implementing the GDPR in the Austria literally hundrets of law were changed; see some of them in § 13.03.D.3.b.
- TKG 2003: (Austrian) Federal Act 2003 enacting a Telecommunications Act and amending the Federal Act on Work Inspection in the Field of Transport and the KommAustria Act.
- ECG: Federal Act that regulates certain legal aspects of electronic commercial and legal transactions (E-Commerce Act).

economic wellbeing of the country, for the prevention of disorder or crime, for the protection of the rights and freedoms of others.”

- UWG: Federal Act Against Unfair Competition of 1984.
- StGB: Austrian Criminal Penal Act.

Definitions and Key Concepts

The text of the GDPR relies on several key terms. These definitions are found primarily in GDPR Art. 4.

Data Subject

A "data subject" is a natural person, identified or unidentifiable. An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier, such as name, an identification number, location data, and an online identifier or by one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity. GDPR Art 4(1).[5]

Data to Be Protected

The law defines several types of data related to a data subject.

Personal Data

"Personal data" is defined as any information relating to an identified or identifiable natural person or "data subject."[6]

The Austrian Supreme Court1, in the context of the admissibility of video-surveillance, also ruled on questions of principle concerning the definition of personal data: The definition of personal data contains three components: A processing component, a content component and an identity component. In the case of image data, the person depicted must at least be recognizable; for this purpose, it is also sufficient that the persons concerned can be identified in retrospect. It is also possible to identify a person if the information is not sufficient in itself to identify a person, but it is possible to do so by linking this information to other information. Recital 26 sentence 3 GDPR also provides that, in determining whether an identifiable person is involved, account should be taken of all the means likely to be used by the person responsible, in accordance with generally accepted practice, to identify the natural person directly or indirectly. It follows from this that the existence of a personal reference can also only arise retrospectively, since the time of processing rather than the time of collection is to be taken into account when determining whether means are likely to be used to identify the natural person according to general discretion.

The Austrian Administrative Supreme Court2 has ruled that e-mails are "personal data": in the case of internal forwarding of e-mails within authorities to staff representatives for the purpose of the reimbursement of travel costs of other staff representatives in order to – in contrast to the processing as an administrative authority – it is another processing operation ("other field of activity") so that it requires a (specific) justification within the meaning of the (now applicable) Art 6 GDPR. Concretely, it was ruled that the forwarding of e-mail communication to other staff representatives was not "necessary", so that the forwarding

[5]GDPR Art 4(1).

[6]GDPR Art. 4(1).

[1] OGH 27.11.2019, 6Ob150/19f.

[2] VwGH 05.06.2020, Ro 2018/04/0023.

constituted a breach of confidentiality interests worthy of protection.

Sensitive Data or Special Categories of Data

Several categories of data, generally known as “sensitive data,” receive special protection. These categories of data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data (when used to uniquely identify a natural person), and data concerning health or a person's sex life or sexual orientation.[7]

Data Relating to Criminal Convictions and Offences

GDPR Provisions.

In addition, under GDPR Art. 10, the processing of data relating to criminal Processing of personal data relating to criminal convictions and offences or related security measures based on GDPR Art. 6(1) may be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. All comprehensive register of criminal convictions must be kept only under the control of official authority.

Austria-Specific Provisions

In Austria, the DSG stipulates that the processing of personal data on acts or omissions punishable by courts or administrative authorities, in particular concerning suspected criminal offences, as well as data on criminal convictions and precautionary measures involving the deprivation of liberty, is permitted if the requirements of the GDPR are met and if (i) an explicit legal authorization or obligation to process such data exists; or (ii) the legitimacy of the processing of such data is otherwise based on statutory duties of diligence, or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party pursuant to GDPR Art. 6(1)(f), and the manner in which the data is processed safeguards the interests of the data subject according the GDPR and the DSG.[8]

Children’s Data

Certain provisions of GDPR recognize the sensitivity of data about children. GDPR Art. 8(1) prohibits the collection and processing of personal data of a child younger than 16 years old. Member States are permitted to change this age limit to between 13 and 16 years.

In Austria, the age threshold is 14.[9]

Data Controllers and Processors

Data Controller

Under the GDPR, a “controller” is a natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of the processing of personal data.[10]

[7]GDPR Art. 9(1).

[8]DSG Section 4(3).

[9]DSG Section 4(4).

[10]GDPR Art. 4(7).

Data Processor

The GDPR defines a "processor" as a natural or legal person, public authority, agency, or another body to which personal data is disclosed, whether the individual or entity is a third party or not.[11]

Austria-Specific Provisions

Pursuant to the Austrian DSG,[12] the statutory right of a Controller to refuse to give evidence may not be circumvented by questioning a Processor working for the Controller and, in particular, not by seizing or confiscating the Controller's documents processed by automated means.

Data Protection Officer

GDPR Provisions

In some circumstances, the GDPR requires data controllers and processors to appoint a "data protection officer (DPO)."[13] The DPO is responsible for informing and advising the data controller or the data processor and any employees who are processing personal data of their obligations under GDPR and for monitoring compliance with GDPR.

Austria-Specific Additional Provisions

The Austrian DSG distinguishes between Public-Sector and Private-Sector Controllers:[14]

Public-Sector Controllers.

- Public-Sector Controllers are all controllers
- That are established in legal structures of public law, in particular also as an executive officer of a territorial authority; or

  As far as they execute laws despite having been incorporated according to private law.

Public-Sector Controllers have the status of a party in proceedings before the Data Protection Authority (DSB). Public-Sector Controllers can lodge complaints with the Federal Administrative Court and final complaints with the Supreme Administrative Court.

Private-Sector Controllers.

Controllers not within the above scope are considered to be Private-Sector Controllers.

Key Government Entities

Several entities have a significant role in the application and implementation of the GDPR.

Supervisory Authority

[11]GDPR Art. 4(8).

[12]DSG Section 6(5).

[13]GDPR Arts. 37 to 39.

[14]DSG Section 26.

GDPR Provisions.

Under GDPR, in each Member State, the activities of data controllers and data processors are overseen by one or more supervisory authorities.[15] Each Member State must have one or more independent public authorities responsible for monitoring the application of the GDPR, protecting the fundamental rights and freedoms of individuals in relation to the processing of their personal data, and facilitating the free flow of personal data within the EU/ European Economic Area (EEA).[16]

Austria-Specific Additional Provisions.

In Austria, the DSG[17] establishes the *Österreichische Datenschutzbehörde* (DSB), which acts as the country's data protection authority.[18]

The DSB is managed by its head. If the head is absent, his or her deputy shall manage the DSB. The rules regarding the head of the DSB shall also apply to the deputy.

Austria Political Advisory Board

The Austrian DSG provides for a "political advisor board", so called Data Protection Council.[19] The Data Protection Council is empowered to comment on questions of fundamental importance for data protection, promote the uniform further development of data protection, and advise the Federal Government on legal policy in the case of projects relevant to data protection.

To fulfil its duties the Data Protection Council (i) can make recommendations relating to data protection to the Federal Government and the federal ministers; (ii) can prepare opinions or commission such opinions; (iii) shall be given the opportunity to comment on draft bills of federal ministries, insofar as these are significant for data protection law, and on regulations to be implemented by the Federal Government concerning essential issues of data protection; (iv) shall have the right to request information and reports from Public-Sector Controllers insofar as this is necessary to evaluate, from the viewpoint of data protection law, projects of significant impact on data protection in Austria; and (v) can publish its observations, concerns and suggestions and submit them to the Public-Sector Controllers.

European Data Protection Supervisor (EDPS)

The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary role is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies. The nature, role, and authority of the EDPS are defined in Regulation (EC) No. 45/2001 (2001).

European Data Protection Board (EDPB)

The supervisory authorities can act independently or as a group as part of the European Data Protection Board (EDPB). The EDPB is composed of the head of one supervisory

[15]GDPR Art. 51.

[16]GDPR Art. 51.

[17]DSG Sections 18 to 23 and 31 to 35.

[18]Website *available at* https://www.dsb.gv.at.

[19]DSG Sections 14 to 17.

authority of each EU Member State and of the European Data Protection Supervisor (EDPS), or their respective representatives.[20]

Territorial Scope

The GDPR applies to entities established in a Member State and, in certain circumstances, to entities that are established elsewhere and process personal data of individuals who are in a Member State.

Entities Established in the EU

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a data controller or a data processor in the EU, whether the processing takes place within the EU or not.[21]

Entities Established Outside the EU

The GDPR may also apply to data controllers and data processors not established in the EU or EEA. This is the case when their processing activities are related to (1) the offering of goods or services to EU/EEA residents, whether or not the activity is connected to a payment; or (2) the monitoring of the behavior of EU residents when their behavior takes place within the EU.[22]

In November 2018, the European Data Protection Board (EDPB) published for consultation Guidelines 3/2018 on the Territorial Scope of GDPR Art. 3.[23]

Main Establishment of Controller or Processor

If a data controller is established in more than one Member State, its main establishment is normally the place of its central administration located in the EU. However, if decisions on the purposes and means of processing of personal data is made in another establishment of the controller in the EU and if that other establishment has power to have such decisions implemented, the establishment making such decisions will be considered as the main establishment.[24]

If a data processor is established in more than one Member State, the main establishment is the place where the processor has its central administration in the EU. If the data processor has no central administration in the EU, the place where the main processing activities take place in the EU will be the main establishment.[25]

[20]GDPR Art. 68.

[21]GDPR Art. 3(1).

[22]GDPR Art. 3(2).

[23]Guidelines are available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.

[24]GDPR Art. 4(16)(a).

[25]GDPR Art. 4(16)(b).

EU Representative

GDPR Art. 4(17) defines a "representative" as a natural or legal person who represents the controller or processor with regard to their respective obligations under the GDPR. When a data controller or data processor is subject to GDPR Art. 3(2), it must designate in writing a representative in the EU, except if the processing is occasional and does not include, on a large scale, processing of special categories of data or data relating to criminal convictions and offenses and is unlikely to result in a risk to the rights and freedoms of individuals.[26]

The representative must be established in one of the Member States where the data subjects whose personal data is processed reside. Its primary role is to receive communications from the data protection supervisory authorities and data subjects on all issues related to the processing of personal data and to ensure compliance with the GDPR.[27]

Principles Relating to the Processing of Personal Data

General Principles

GDPR Art. 5(1) sets forth six principles governing the processing of personal data.

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation:** Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data Minimization:** Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed.
- **Accuracy:** Personal data must be accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate in regard to the purpose for which they are processed are erased or rectified without delay.
- **Storage Limitation:** Personal data must be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data is processed.
- **Integrity and Confidentiality:** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Accountability

The six principles are supplemented with a separate requirement for accountability. Under the accountability principle of GDPR Art. 5(2), the data controller is responsible for compliance with the six principles outlined above. The data controller is expected to be able to demonstrate compliance with those six principles.

[26]GDPR Art. 27.

[27]GDPR Art. 27.

Lawfulness of Processing

GDPR Provisions

Lawfulness of the processing is a key principle of the GDPR. GDPR Art. 6(1) establishes the conditions for lawful processing for personal data. Under GDPR Art. 6(2), Member States may introduce additional provisions.

Under GDPR Art. 6(1), the processing of personal data (other than special categories of data, which are subject to special rules) is lawful only in six circumstances.

- **Consent:** The data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
- **Contract:** Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which the controller is subject;
- **Vital Interest:** Processing is necessary to protect the vital interests of the data subject or another individual;
- **Public Interest:** 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 data controller; or
- **Legitimate Interest:** Processing is necessary to the purposes of the legitimate interests pursued by the controller or by a third party, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular when the data subject is a child.

Austria-Specific Additional Provisions

The Austrian DSG includes additional rules on the legitimate data processing for specific purposes.

Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes.[28]

For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes whose goal is not to obtain results in a form relating to specific data subjects, the controller may process all personal data that

- Is publicly accessible;
- The controller has lawfully collected for other research projects or other purposes; or
- Is pseudonymized personal data for the controller, and the controller cannot establish the identity of the data subject by legal means.

[28]DSG Section 7.

In the case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes that do not fall under the above framework, personal data may be processed only

- Pursuant to specific legal provisions;
- With the consent of the data subject; or
- With a permit of the DSB.

A permit of the DSB for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is granted at the request of the Controller ordering the research project, if

- The consent of the data subject is impossible to obtain because the data subject cannot be reached, or the effort would otherwise be unreasonable;
- There is a public interest in the processing for which a permit is sought; and
- The professional aptitude of the controller has been satisfactorily demonstrated.

If special categories of personal data (as defined in GDPR Art. 9) are to be collected, an important public interest in the research project must exist. In addition, it must be ensured that the personal data is processed at the premises of the controller ordering the research project only by persons who are subject to a statutory obligation of confidentiality regarding the subject matter of the research project or whose reliability in this respect is credible. The DSB shall issue the permit subject to terms and conditions, insofar as this is necessary to safeguard the data subjects' interests which deserve protection.

Even in cases where the processing of personal data for scientific research purposes or statistical purposes is permitted in a form which allows the identification of data subjects, the data must be pseudonymized without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistical work can be performed with pseudonymized personal data. Unless otherwise expressly provided for by law, data in a form that allows the identification of data subjects must be rendered unidentifiable as soon as it is no longer necessary for scientific or statistical work to keep them identifiable.

The Data Protection Authority approved[3] the application of a research institute from 24th July 2019 for the granting of a license under § 7 (3) Data Protection Act as follows: The applicant is granted permission to determine and process personal data for the purpose of developing test data for algorithms in the area of (partially) autonomous driving in the course of image recordings in public places within Austria from the perspective of the driver of road or rail vehicles. In order to safeguard the legitimate interests of the data subjects, the following conditions are imposed: (a) the vehicles carrying out the recordings must be marked in such a way that the identity of the applicant is disclosed and those affected are informed where they can obtain information in accordance with Art 13 GDPR; (b) the access to image recordings containing personal data must be secured by the applicant in a suitable manner in accordance with Art 32 (1) GDPR, e.g. by means of a seal (for recordings on paper) or a password (for electronic recordings); (c) the inspection and evaluation of the image recordings may only be carried out by certain trained employees of the applicant or his processor who are informed about § 6 Data Protection Act and whose reliability in handling data is guaranteed in accordance with § 6 (3) Data Protection Act; (d) publication of the image data may only take place in anonymous form; (e) a transfer of image data within the framework of cooperation

[3] DSB 21.01.2020, DSB-D202.235.

agreements may only be made to scientific institutions which are also researching the development of secure algorithms for (partially) autonomous driving or which provide credible assurances of this, exclusively for research purposes in this area. Only such image data may be transmitted where the interests of identifiable persons requiring the protection of personal data do not outweigh the interests of applicants or other scientific institutions in developing secure algorithms for (partially) autonomous driving. Image data may only be transferred to scientific institutions in third countries without an adequate level of data protection if standard contractual clauses within the meaning of Art 46 (2) (c) GDPR are concluded.

Legal restrictions on the right to use personal data for other reasons, in particular for copyright reasons, shall not be affected.

Processing for Providing Addresses to Inform and Interview Data Subjects.[29]

Unless otherwise expressly provided for by law, providing address data of a certain group of data subjects in order to inform or interview them requires the consent of the data subjects. If, however, an infringement of the data subject's interests in confidentiality is unlikely, considering the selection criteria for the group of data subjects and the subject of the information or interview, no consent shall be required (i) if data from the same controller are processed, or (ii) in the case of an intended transfer of address data to third parties, (a) if there is also a public interest in the information or interview, or (b) if none of the data subjects, after having received appropriate information on the reason and content of the transfer, has objected to the transfer within a reasonable period.

If the requirements are not met and if obtaining the consent of the data subjects would require a disproportionate effort, the transfer of the address data is permissible with a permit of the DSB if the data is to be transferred to third parties:

- For the purpose of information or an interview due to an important interest of the data subject;
- Due to an important public interest in the information or interview; or
- For an interview of the data subjects for scientific or statistical purposes.

The DSB must grant the permit for the transfer of personal data at the request of a controller processing address data, if the controller has satisfactorily demonstrated that the requirements have been met and no overriding interests in confidentiality that deserve protection on the part of the data subjects represent an obstacle to the transfer.

The DSB must issue the permit subject to terms and conditions, insofar as this is necessary to safeguard the data subjects' interests that deserve protection. The transferred address data may only be processed for the permitted purpose and must be erased as soon as they are no longer needed for information or interviews.

If it is lawful pursuant to the aforementioned provisions to transfer the names and addresses of persons belonging to a certain group of data subjects, the processing required for selecting the address data to be transferred must also be permitted.

[29]DSG Section 7.

Processing and Freedom of Expression.[30]

If it is necessary to reconcile the right to the protection of personal data with the freedom of expression and information, in particular with regard to the processing of personal data by media undertakings, media services and their employees directly for their journalistic purposes as referred to in the Media Act, Chapter II (principles), with the exception of Article 5, Chapter III (rights of the data subject), Chapter IV (controller and processor), with the exception of Articles 28, 29 and 32, Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency), and Chapter IX (specific data processing situations) of the GDPR shall not apply to processing for journalistic purposes or the purposes of academic, artistic or literary expression.

Of the provisions of the DSG Section 6 ("Confidentiality of Data") shall be applied in such cases.

Processing of Personal Data in Case of Emergency.[31]

In case of emergency, Public-Sector Controllers and relief organizations shall be authorized to jointly process data to the extent that this is necessary to assist persons directly affected by a disaster, to locate and identify missing or deceased persons and to provide information to their relatives.

Anybody who lawfully possesses personal data shall be permitted to transfer these data to Public-Sector Controllers and relief organizations if these controllers and organizations need this personal data to manage a disaster.

The transfer abroad of personal data is permitted insofar as this is absolutely necessary to fulfil above purposes. Data that by themselves would make the data subject liable to criminal prosecution shall not be transferred unless they are absolutely necessary for identification in a particular case. The DSB shall be informed immediately about the data transfers performed and about the circumstances of the motivating incident. The DSB shall prohibit further data transfers if the interference with the fundamental right to data protection resulting from the data transfer is not justified by the special circumstances caused by a disaster.

Based on a specific inquiry of a close relative of a person who has actually or presumably been directly affected by a disaster, Controllers are authorized to transfer to the inquiring person personal data regarding the whereabouts of the data subject and on the progress of the search, if the relative satisfactorily demonstrates his or her identity and close relationship to the data subject.

Special categories of personal data (GDPR Art. 9) may be transferred to close relatives only if they prove their identity and their capacity as a relative and if the transfer is necessary to safeguard their rights or the rights of the data subject. The social insurance agencies and authorities are obliged to assist the Public-Sector Controllers and relief organizations if this is necessary to verify the information provided by the inquiring person.

Close relatives pursuant to this provision means parents, children, spouses, registered partners and companions in life of the data subjects. Other relatives may receive the aforementioned information under the same conditions as close relatives if they satisfactorily

[30]DSG Section 9.

[31]DSG Section 10.

demonstrate a special close relationship to the person actually or presumably directly affected by a disaster.

The personal data processed for the purposes of managing a disaster shall be deleted immediately if they are no longer required to fulfil the specific purpose.

Consent as Basis for Lawful Processing

GDPR Art. 6(1)(a) allows the processing of personal data when "the data subject has given consent to the processing or his or her personal data for one or more specific purposes." GDPR Art. 4(11) defines consent 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."

GDPR Art. 7(1) defines the conditions for consent and states that, where processing is based on consent, a controller must be able to demonstrate that the data subject has consented to the processing of his or her data.

GDPR Article 7(2) provides that the request for consent must be presented in a matter that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. GDPR Art. 7(3) grants the data subjects the right to withdraw their consent at any time.

Legitimate Interest as a Legal Basis for Processing

GDPR Art. 6(1)(f) allows the processing of personal data when it is necessary "for the purposes of the legitimate interest of the data controller or by a third party." However, this legitimate interest must be balanced against the interest of the individuals. Processing for the legitimate interest of the controller or a third party must not override the interests or the fundamental rights and freedoms of the data subjects that require protection of personal data. The analysis must take into account the data subjects' reasonable expectations based on their relationship with the controller and balance the interest of the controller.[32]

The Austrian Administrative Supreme Court[4] has ruled that in the case of internal forwarding of e-mails within authorities to staff representatives for the purpose of the reimbursement of travel costs of other staff representatives in order to – in contrast to the processing as an administrative authority – it is another processing operation ("other field of activity") so that it requires a (specific) justification within the meaning of the (now applicable) Art 6 GDPR. Concretely, it was ruled that the forwarding of e-mail communication to other staff representatives was not "necessary", so that the forwarding constituted a breach of confidentiality interests worthy of protection.

The DSB[5] hat zur Frage, ob die Österreichische Post den Beschwerdeführer dadurch in seinem Recht auf Geheimhaltung verletzt hat, indem ein Mitarbeiter im Zuge der Abholung einer Postsendung (Einschreibsendung) Ausweisdaten elektronisch erfasst und gespeichert hat: Die DSB kam zum Ergebnis, dass es keine gesetzliche Grundlage für das Scannen und Speichern des Ausweises gibt; die Allgemeinen Geschäftsbedingungen selbst können mangels materieller Rechtsqualität keine rechtliche Verpflichtung im Sinne der DSGVO sein.

[32] GDPR, Preamble § 47.

[4] VwGH 05.06.2020, Ro 2018/04/0023.

[5] DSB 26.06.2020, 2020-0.349.984.

Hingegen hat die Österreichische Post ein berechtigtes Interesse im Sinne der DSGVO, sich im Falle eines Rechtsstreits hinreichend, zumindest innerhalb der gesetzlichen Gewährleistungsfrist, verteidigen und den Nachweis der rechtmäßigen Übergabe an die korrekte Person erbringen zu können. Damit aufgrund dieses berechtigten Interesses der Post die Verarbeitung der Ausweisdaten rechtmäßig ist, war dieses dem Geheimhaltungsanspruch des Beschwerdeführers gegenüberzustellen und ein allfälliges Überwiegen zu prüfen: Dabei ist unter anderem auch auf die vernünftigen Erwartungen des Beschwerdeführers abzustellen, also insbesondere, ob er zum Zeitpunkt der Erhebung der Ausweisdaten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen konnte, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird (vgl. ErwG. 47 DSGVO). Die Erfassung und Speicherung der Ausweisdaten zum Zwecke der Verteidigung von Rechtsansprüchen betreffend Postsendungen liegt jedenfalls innerhalb der allgemeinen Lebenserfahrung und war insoweit für den Beschwerdeführer auch leicht absehbar. Die verarbeiteten Datenkategorien sind keinesfalls überschießend und ist auch die Speicherdauer mit sechs Monaten keinesfalls als unverhältnismäßig anzusehen.

Processing of Special Categories of Data

Different rules apply to the processing of “special categories of data.” These special categories of data includes personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; the processing of genetic data or biometric data in order to uniquely identify a natural person; and data concerning health or a person's sex life or sexual orientation.

The processing of data that meet the definition of special categories of data is prohibited, except in 10 cases listed in GDPR Art. 9(2). These exceptions include the following:

- **Explicit Consent:** The data subject has given explicit consent to the processing except where EU or Member State law provides that the prohibition may not be lifted by the data subject;
- **Employment, Social Protection**: The processing is necessary for carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment, social security, and social protection law insofar as it is authorized by EU or Member State law or by a collective agreement;
- **Vital Interest:** The processing is necessary to protect the vital interests of the data subject or another individual when the data subject is physically or legally incapable of giving consent;
- **Nonprofit Body:** The processing is carried out in the course of legitimate activities by a foundation, association, or nonprofit entity; relates solely to that entity's members or former members; and the data is not disclosed to others without the consent of the data subjects;
- **Data Already Made Public:** The processing relates to personal data that are manifestly made public by the data subject;
- **Exercise of Defense of Legal Claims:** The processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity;
- **Substantial Public Interest:** The processing is necessary for reasons of substantial public interest on the basis of EU or Member State law that must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable measures to safeguard the fundamental rights and interests of the data subject;

- **Health, Diagnosis, Social Care:** The processing is necessary for preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or pursuant to a contract with a health professional;
- **Public Health:** The processing is necessary for reasons of public interest in the area of public health, subject to appropriate protection and professional secrecy;
- **Archiving and Research:** The processing is necessary for archiving purposes in the public interest, scientific and historical research, or statistical purposes based on EU or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

Austrian Case Law on Processing of Political Opinion

In aufsehenerregenden Entscheidungen gegen die Österreichische Post zur Verarbeitung von statistischen Daten zur „Parteienaffinität“ (auch weil sie mit Geldbußen in der Höhe von EUR 18 Mio einhergingen) gehen die Datenschutzbehörde und das Bundesverwaltungsgericht (20.08.2020, W258 2217446-1) von einer sehr weiten Anwendung des Art. 9 DSGVO aus: Strittig war, ob aus dem Datum, dass sich eine Person mit einer gewissen Wahrscheinlichkeit für Werbung über eine bestimmte politische Partei interessiert, die politische Meinung dieser Person im Sinne des Art 9 Abs 1 DSGVO hervorgeht. Die Datenschutzbehörde und das Gericht urteilte: Auf Grund des Wortlauts des Art 9 Abs 1 DSGVO, wonach das Verbot die Verarbeitung als solche betrifft, kommt es dabei lediglich auf die grundsätzliche Eignung der Datenarten an, diese Gefahren auszulösen. Der konkrete Verarbeitungskontext, wie Zweck der Verarbeitung oder konkrete Verarbeitungsschritte, sind somit für die Qualifikation als „sensible Daten“ irrelevant. Da bereits eine vermutete politische Meinung jene negativen Folgen für die betroffene Person auslösen kann, vor der Art 9 DSGVO schützen möchte, ist es für die Annahme einer politischen Meinung ausreichend, wenn aus der Information eine solche Meinung mit hinreichender Wahrscheinlichkeit hervorgeht. Gewissheit ist nicht erforderlich. Irrelevant ist auch, ob die Merkmalsangaben inhaltlich zutreffen. Ob aus personenbezogenen Daten die politische Meinung der betroffenen Person mit hinreichender Wahrscheinlichkeit hervorgeht, ist aus dem Umständen des Einzelfalls unter Berücksichtigung des Schutzzwecks der Norm zu beurteilen.

Austrian Case Law on Processing of Health Data

Die DSB (12.06.2020, 2020-0.225.643) hat zur Frage der Rechtmäßigkeit der Verarbeitung von Rechnungen der Apotheken bzw. Ärzte durch Versicherungen abgesprochen: Der Beschwerdeführer vermeint, dass zur Auszahlung der Versicherungsleistung die Übermittlung einer Rezeptgebührenbestätigung ausreiche und er durch das Einreichen der saldierten Originalrechnungen in seinem Recht auf Geheimhaltung verletzt werde, da die Versicherung dadurch Kenntnis über die ihm verschriebenen Medikamente – und indirekt damit über seinen Gesundheitszustand – erlange. Die Verarbeitung von Gesundheitsdaten im Kontext des Versicherungsrechts richtet sich nach § 11a VersVG, gemäß dessen Abs. 1 der Versicherer im Zusammenhang mit Versicherungsverhältnissen, bei welchen der Gesundheitszustand des Versicherten oder eines Geschädigten erheblich ist, personenbezogene Gesundheitsdaten verarbeiten darf, soweit dies zur Verwaltung bestehender Versicherungsverträge (Z 2) oder zur Beurteilung und Erfüllung von Ansprüchen aus einem Versicherungsvertrag (Z 3) unerlässlich ist. § 34 VersVG verpflichtet den Versicherungsnehmer zur Erteilung von

Auskünften an den Versicherer, wenn dies zur Feststellung des Versicherungsfalles oder des Umfanges der Leistungspflicht des Versicherers erforderlich ist. Nur in seltenen Ausnahmefällen wird es dem Versicherungsnehmer nicht zumutbar sein, Urkunden, die sich in seiner Verfügungsbefugnis befinden, vorzulegen. Es erscheint auch „denkmöglich", dass die Versicherung die Originalrechnungen für die Beurteilung des maßgeblichen Sachverhalts, nämlich des genauen Umfangs ihrer Leistungspflicht, benötigt.

Das Bundesverwaltungsgericht urteilte am 28.05.2020, W211 2216385-1, über die Beschwerde des Beschwerdeführers (eines Lehrers) wonach durch die Offenlegung und Übermittlung von Gesundheitsdaten, nämlich der Krankengeschichte samt psychiatrischem Gutachten, an Unbefugte (im Rahmen eines vom Lehrer angestrengten Aufsichtsverfahrens gegen andere Lehrer) dieser in seinem Grundrecht auf Datenschutz verletzt worden sei. Wesentlicher Punkt der Dienstaufsichtsbeschwerde war das Mobbinggeschehen am Arbeitsplatz infolgedessen es zu den Gesundheitsproblemen des Lehrers kam. Das Gericht sah dadurch, dass die Gesundheitsdaten des Lehrers an alle Beteiligten übermittelt wurden, dessen Grundrecht auf Datenschutz verletzt: die beteiligten Personen waren ausschließlich dazu aufgefordert, zu den faktischen Geschehnissen rund um die Mobbingvorwürfe Stellung zu nehmen; dass sie außerdem – insbesondere auf Basis der Krankenunterlagen des Lehrers – Aussagen zu den (möglichen) gesundheitlichen Folgen hätten treffen können oder sollen, ist den Verfahrensergebnissen des Aufsichtsverfahrens nicht zu entnehmen. Das Weglassen der Gesundheitsdaten wäre ohne Schwierigkeiten möglich gewesen. Auch konnte – obschon der Lehrer die Gesundheitsdaten seiner Sachverhaltsdarstellung zur Einleitung des Aufsichtsverfahrens angeschlossen hatte – nicht von einer ausdrücklichen Einwilligung ausgegangen werden; eine solche hat unzweideutig zu erfolgen, wonach der betroffenen Person die beabsichtigte Verarbeitung und der Zweck mitzuteilen ist und die Einwilligung derart zu gestalten ist, dass über deren Erteilung kein Zweifel besteht. Weder wurde dem Beschwerdeführer die Übermittlung der gesundheitsbezogenen Beilagen mitgeteilt, noch wurde seine Einwilligung dazu eingeholt.

Der Beschwerdeführer beantragte in obiger Beschwerde auch die Löschung der Gesundheitsdaten bei den Empfängern. Diesbezüglich entschied das Gericht, dass das Löschungsbegehren des Beschwerdeführers als ein Mittel, das geeignet scheint, den rechtsverletzenden Zustand zu sanieren, bzw. einen datenschutzrechtlich konformen Zustand wiederherzustellen. Dass eine weitere Aufbewahrung auch zur Wahrung allfälliger Rechtsansprüche erforderlich wäre, verneinte das Gericht. Andere Gründe, die einer Löschung entgegenstehen könnten, kamen im Verfahren nicht hervor, weshalb die weitergegebenen und übermittelten Beilagen der Dienstaufsichtsbeschwerde (mit den Gesundheitsdaten des Lehrers) zu löschen bzw. zu vernichten sind. Seitens des erkennenden Senats wird dabei nicht übersehen, dass es sich bei der mitbeteiligten Partei um eine Verantwortliche des öffentlichen Rechts handelt, und sich daher die Frage eines Konflikts mit § 24 Abs. 5 DSG, wonach nach dieser Bestimmung die Erlassung eines Leistungsbescheids gegenüber Verantwortlichen des öffentlichen Rechts nicht möglich sein soll, stellt. Diese nationale Regelung erscheint jedoch im Lichte der DSGVO, deren Ziel die Schaffung eines einheitlichen europäischen Datenschutzrechts sowohl im privaten wie auch im öffentlichen Bereich und seine umfassende und wirksame Anwendung ist, nicht haltbar. Daher können – entgegen dem Wortlaut des österreichischen Gesetzes – auch gegenüber Behörden Leistungsbescheide durch die Datenschutzbehörde erlassen werden.

Processing of Personal Data About Children

Under GDPR Art. 8, the processing of personal data of a child is lawful only to the extent

that consent is given by the holder of parental responsibility over the child and the controller has made reasonable efforts to verify, in such cases, that the consent is given by the holder of the parental responsibility over the child, taking into consideration available technology.[33]

GDPR Art. 8 requires each Member State to identify the age thresholds for the processing of child information. In Austria, the processing of personal data of the child is legal if the child is at least 14 years of age,[34] and the remainder of the requirements for the processing of personal data under GDPR are fulfilled.

Processing of Personal Data About Criminal Convictions and Offenses

GDPR Provisions

GDPR Art. 10 focuses on the processing of personal data relating to criminal convictions and offenses. It provides that the processing of personal data relating to criminal convictions and offenses, as defined under GDPR Art. 6(1), may be carried out only under the control of official authority or when authorized by specific by EU or Member State law. Further, any comprehensive register of criminal convictions may be kept only under the control of official authorities.

Austria-Specific Additional Provisions

In Austria, the DSG stipulates that the processing of personal data on acts or omissions punishable by courts or administrative authorities, in particular concerning suspected criminal offences, as well as data on criminal convictions and precautionary measures involving the deprivation of liberty, is permitted if the requirements of the GDPR are met and if:

- There is an explicit legal authorization or obligation to process such data; or
- The legitimacy of the processing of such data is otherwise based on statutory duties of diligence; or
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party pursuant to GDPR Art. 6(1)(f); and
- The manner in which the data is processed safeguards the interests of the data subject according to the GDPR and the DSG.[35]

Rights of Data Subjects

Overview

Data subjects are granted a wide variety of rights, including the following rights:

- Information

[33]GDPR Art. 8(2).

[34]DSG Section 4(4).

[35]DSG Section 4(3).

- Access
- Rectification
- Erasure
- Restriction of processing
- Portability
- Objection
- Not to be subject to automated decisions, including profiling

GDPR Art. 12(3) requires controllers to respond to a data subject's request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, and the controller must inform the data subject of any such extension within one month of receipt of the request and provide the reasons for the delay. Where the data subject makes the request by electronic means, the information must be provided by electronic means where possible, unless the data subject requests otherwise.

The Austrian DSB provides several forms to facilitate data subject's requests (also in the English language).[36]

Please note that—although the data subject's rights are focused on natural person's rights—in Austria, also legal entities have data subject's rights, which however cannot be enforced via the Austrian DSB, but only via the civil courts. The Austrian law provides the "Fundamental Right To Data Protection":[37] Every person [including legal entities] shall have the right to secrecy of the personal data concerning that person, especially with regard to the respect for his or her private and family life, insofar as that person has an interest which deserves such protection.

Such an interest is precluded if data cannot be subject to the right to secrecy due to the general availability of the data, or because the data cannot be traced back to the data subject.

Insofar as personal data concerning a person is intended for automated processing or processing in files managed manually, i.e. files managed without automated processing, every person shall, as provided for by law, have (i) the right to obtain information as to who processes what data concerning the person, where the data originated from, for which purpose they are used, and in particular to whom the data is transmitted; (ii) the right to rectification of incorrect data and the right to erasure of illegally processed data.

Right to Information

The right to information includes the right to obtain from the controller confirmation as to whether personal data concerning the data subject are being processed; when that is the case, the individual also has the right to information about details of the processing, including the

- Purpose;
- Categories of personal data concerned;

[36]https://www.dsb.gv.at/dokumente (in German language).

[37]DSG Section 1.

- Categories of recipients to whom the personal data have or will be disclosed;
- How long the data will be stored;
- The existence of the right to request rectification or erasure; restriction to the processing of personal data concerning the data subject, or to object to such processing;
- The existence of the right to lodge a complaint with the supervisory authority;
- Information about the source of the personal data;
- Information about the existence of automated decision making, including profiling; and
- Information about the transfer of personal data to a third country, and the safeguards used for such transfer.

Right of Access

GDPR Provisions

The right of access means the right to receive a copy of the personal data undergoing the processing. Where the request is made by electronic means, the information must be processed in a commonly used electronic form.[39]

Austria-Specific Additional Provisions and Case Law

The Austrian DSG stipulates[40] that without prejudice to other legal restrictions, the data subject does not have the Right of Access:

- if this access jeopardizes the fulfillment of a task legally assigned to the Controller; or
- if this access would endanger a business or trade secret of the Controller or third parties.

The Federal Administrative Court has – which is also relevant for the question of the right of information pursuant to Art. 15 GDPR and also its restriction in § 4 (6) Data Protection Act – decided:[6] With the Beneficial Owners Register Act (BORA), a register was set up in which the beneficial owner of companies, other legal persons and trusts are registered. The area of application of the Beneficial Owners Register Act (from hereinafter: Register) was specified by binding law through Art 30 and 31 of the Directive (EU) 2015/849 (4. Money Laundering Directive) and subsequently amended by the Directive (EU) 2018/843 (5. Money Laundering Directive). The Directive 2018/843 also provides for public access to information regarding beneficial owners, which enables a greater control of information through civil society (including the press and civic organizations), and the trust in the integrity of the operations and the financial system is strengthened. Furthermore, the member states should have the possibility, with the goal of ensuring an appropriate and balanced approach and for the preservation of the right to private life and the protection of personal data, to provide for exemptions from the obligation for registers to disclose information on the beneficial owner and from the possibility of accessing such information in exceptional circumstances, in which the beneficial owner would be subjected to a disproportionate risk of fraud, kidnapping, extortion,

[39] GDPR Art. 15(3).

[40] DSG Sections 4(5) and (6).

[6] BVwG 11.05.2020, W195 2226816-1/9E.

racketeering, harassment, violence or intimidation through the information (see Directive 2018/843 (EU), (36)); the Austrian legislator has taken this into account in § 10a BORA under the title “Limitation of Access in Exceptional Circumstances”: The limitation option available is intended to prevent beneficial owners from becoming victims of fraud, blackmail, kidnapping, extortion, criminal offences against life and limb, coercion, dangerous threats or persistent persecution. It is to be assumed that the legislator assumes and that it was also provided for the purposes of the Directive that such threatened or criminal offences committed do not constitute mandatory requirements to consider a limitation to be permissible and only in the case of the commission of an offence of such gravity, this circumstance must be regarded as 'exceptional' in the individual case.

The Federal Administrative Court decided on the Right of Access on a Google-case as following hinsichtlich Fragen zur Rechtsnachfolge des Verantwortlichen bzw. hinsichtlich der Identifizierbarkeit von Auskunftswerbern und zu Online-Werkzeugen zur Auskunftserteilung:[7] Der Beschwerdeführer erhob am 01.02.2016 eine Datenschutzbeschwerde gegen Google Inc. (= Beschwerdegegnerin vor der Datenschutzbehörde und mitbeteiligte Partei vor dem Bundesverwaltungsgericht) wegen Verletzung im Recht auf Auskunft.

- Die Datenschutzbehörde hat in der Verhandlung vor dem Bundesverwaltungsgericht die Meinung vertreten, dass – aufgrund der erfolgten Organisations- bzw. Unternehmensänderung innerhalb von Google – nicht mehr Google Inc. (nunmehr Google LLC), sondern Google Ireland Limited zur Erteilung der gegenständlichen Auskünfte an den Beschwerdeführer zuständig sei. Das Bundesverwaltungsgericht sprach aber aus, dass sich die Frage der Verantwortlichkeit ausschließlich auf den Zeitraum (hier: Eingang des Auskunftsbegehrens vom 30.10.2015 bis 24.02.2016), in dem die Tat einer allfälligen Datenschutzverletzung begangen wurde, bezieht. Jede andere Interpretation – so auch obige der Datenschutzbehörde – würde zu dem sinnwidrigen Ergebnis führen, dass eine juristische Person als Verantwortliche (Täterin) sich durch eine nachträgliche Änderung ihrer Organisations- bzw. Unternehmensstruktur ihrer Verantwortlichkeit für die Tat einer Datenschutzverletzung (im Verwaltungsstrafverfahren ihrer strafrechtlichen Verfolgung) entziehen könnte.

- Zur Frage der Identifizierbarkeit ist auch auf die Rechtsprechung des Verwaltungsgerichtshofes zu verweisen, wonach die Identität einer betroffenen Person auch aus der Situation heraus klar sein kann. Dies kann beispielsweise der Fall sein, wenn sich der Auftraggeber (Anm.: nunmehr Verantwortliche) – ohne an der Identität des Betroffenen zu zweifeln – nach einem unmittelbar vorangegangenen Rechtsstreit bereits auf eine längere Korrespondenz mit diesem eingelassen hat (VwGH v. 04.07.2016, Ra 2016/04/0014; siehe auch BVwG v. 27.05.2020, Zl. W214 2228346-1/16E).

- Zum Verweis auf Einsicht der Online-Werkzeuge versus Schriftlichkeit betreffend personenbezogener Daten innerhalb des Nutzerkontos: Der Verweis auf die Einsicht der Online-Werkzeuge des Nutzerkontos wurde bereits von der DSB hinsichtlich der dort abrufbaren personenbezogenen Daten als rechtens gewertet. Dazu hat der Beschwerdeführer in seiner Stellungnahme geltend gemacht, dass nach der DSGVO nur dann, wenn Auskunftswerber Auskunftsverlangen elektronisch stellen, Auskünfte in einem gängigen elektronischen Format erteilt werden könnten; doch selbst in diesem Fall können Auskunftswerber eine schriftliche Auskunftserteilung verlangen. Aus Sicht des erkennenden Senates ist dem aber entgegenzuhalten: Der Beschwerdeführer ist Computer versiert und hat zuhause ein Computerequipment; er hat auch in der

[7] BVwG 23.09.2020, W101 2132039-1.

> Verhandlung nicht bestritten, aufgrund seiner Computerausstattung grundsätzlich die Möglichkeit zu haben, in die Online-Werkzeuge seines Nutzerkontos Einsicht zu nehmen. In diesem Zusammenhang gilt es außerdem zu berücksichtigen, dass im Erwägungsgrund (63) ausdrücklich erwähnt wird: Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Aus diesen Erwägungen folgt für den vorliegenden Fall, dass der Beschwerdeführer als Inhaber eines Nutzerkontos bei der mitbeteiligten Partei die Möglichkeit hatte, Einsicht in die Online-Werkzeuge zu nehmen, und er insofern nicht berechtigt ist, neben dieser Art der Auskunftserteilung zusätzlich Auskünfte zu den personenbezogenen Daten innerhalb seines Nutzerkontos in schriftlicher Form zu bekommen. Daher muss sich der Beschwerdeführer hinsichtlich dieser personenbezogenen Daten auf die Einsicht in die Online-Werkzeuge verweisen lassen.

Das Bundesverwaltungsgericht sprach zur Identifizierbarkeit bei Auskunftsbegehren folgendes aus (27.05.2020, W214 2228346-1): Der Auskunftsanspruch setzt gemäß Art. 12 DSGVO unter anderem voraus, dass die Identität des Auskunftswerbers feststeht. Bei begründeten Zweifeln an der Identität kann der Verantwortliche zusätzliche Informationen anzufordern, die zur Bestätigung der Identität erforderlich sind. Dass dadurch jedoch keine routinemäßige Identitätsprüfung ermöglicht wird und ein Verantwortlicher daher nicht generell die Vorlage eines Identitätsnachweises verlangen darf, wird in der Beschwerde von der Beschwerdeführerin ausdrücklich zugestanden. Die Beschwerdeführerin vermeint jedoch, dass Zweifel an der Identität nicht durch die bloße Bekanntgabe einer E-Mail-Adresse oder Postanschrift zerstreut werden könnten. In ihrer Argumentation übersieht die Beschwerdeführerin jedoch, dass sie im Verfahren zu keinem Zeitpunkt - weder in der Kommunikation mit dem Mitbeteiligten, noch im Verfahren vor der belangten Behörde oder in ihrer Beschwerde - dargelegt hat, aus welchem Grund sie an der Identität des Mitbeteiligten zweifelt. Der Mitbeteiligte hat ausdrücklich nachgefragt, ob derartige begründete Zweifel gegeben seien und bejahendenfalls, worin diese bestünden, bekam aber keine diesbezügliche Antwort. Wie die belangte Behörde und der Mitbeteiligte zutreffend ausgeführt haben, sind der Beschwerdeführerin der vollständige Name, die Adresse und E-Mail-Adresse des Mitbeteiligten bekannt und hat der Mitbeteiligte sein Auskunftsbegehren auch mit einer qualifizierten elektronischen Signatur versehen. Der Vollständigkeit halber: Die DSB kann daher auch gegenüber Verantwortlichen des öffentlichen Bereiches einen Leistungsbescheid erlassen (entgegen dem Wortlaut des § 24 DSG).

Weiters entschied das Bundesverwaltungsgericht zum Verhältnis der Auskunftspflicht der mit Aufgaben der Bundesverwaltung betrauten Organe (Art 20 Abs 4 B-VG und Auskunftspflichtgesetz), der Amtsverschwiegenheit und dem Datenschutzrecht:[8] Die Auskunft ist zu erteilen, soweit eine gesetzliche Verschwiegenheitspflicht dem nicht entgegensteht. Um beurteilen zu können, ob einem nach dem Auskunftspflichtgesetz gestellten Auskunftsbegehren 'verfassungsrechtlich verankerte Prinzipien datenschutzrechtlicher Geheimhaltung und damit das im Art. 20 Abs. 3 B-VG enthaltene Gebot der Amtsverschwiegenheit im überwiegenden Interesse einer Partei' entgegensteht, bedarf es konkreter sachverhaltsbezogener Feststellungen darüber, ob es sich bei den, den Gegenstand der Anfrage bildenden Daten um solche personenbezogener Art handelt und welche schutzwürdigen Interessen diese Person an der Geheimhaltung dieser Daten hat, und schließlich allenfalls, ob und welche berechtigten Interessen eines/einer Auskunftswerbers/Auskunftswerberin an einer Bekanntgabe dieser Daten bestehen. Auf Grund des so ermittelten Sachverhaltes ist es sodann Sache der Behörde im Rechtsbereich

[8] BVwG 23.09.2020, W101 2132039-1; vgl auch 15.05.2020, W211 2211099-1 (ASFINAG)

zu beurteilen, ob die Tatbestandsvoraussetzungen des DSG erfüllt sind und, sofern diese Frage zu bejahen ist, ob das Interesse eines/einer Auskunftswerbers/Auskunftswerberin an der begehrten Auskunft dieses Geheimhaltungsinteresse überwiegt (vgl. VwGH 22.10.2012, 2010/03/0099).

Das Bundesverwaltungsgericht entschied am 28.05.2020 zu W274 2224656-1 zum Ablehnungsrecht und auch zu allgemeinen Grundsätzen bei Auskunftsbegehren: Gemäß Art. 57 Abs. 4 DSGVO kann die Aufsichtsbehörde bei offenkundig unbegründeten oder - insbesondere im Falle einer häufigen Wiederholung - exzessiven Anfragen, eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage. Eine Weigerung bedeutet aber nicht, dass die Aufsichtsbehörde eine Anfrage einfach ignorieren darf. Sie kann sich bloß weigern, inhaltlich tätig zu werden. Zumindest bei offenkundig unbegründeten Anfragen wird zunächst ein Verbesserungsauftrag zu erteilen sein. Nach fruchtlosem Ablauf der von der DSB zu setzenden Frist für die Verbesserung kann die Anfrage per Beschluss zurückgewiesen werden. Das Recht auf Auskunft nach Art 15 DSGVO ist zentraler Bestandteil des Selbstdatenschutzes und ermöglicht der betroffenen Person Grundlegendes über die Verarbeitung ihrer Daten zu erfahren, insb ob und welche Daten der Verantwortliche über sie verarbeitet, und ob dies rechtmäßig geschieht. Jedoch hat der österr Gesetzgeber zwei Ausnahmen für das Auskunftsrecht selbst vorgesehen: Nach § 4 Abs 5 DSG besteht bei hoheitlich tätigen Verantwortlichen das Recht auf Auskunft nicht, wenn durch die Erteilung der Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird. § 4 Abs 6 DSG schließt das Auskunftsrecht "in der Regel" aus, wenn die Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen oder eines Dritten gefährden würde. Die betroffene Person muss ihren Anspruch auf Auskunft dem Verantwortlichen gegenüber geltend machen (Art 15 Abs 1). Der Auftragsverarbeiter ist nach Art 28 Abs 3 lit e vertraglich zu verpflichten, dass er den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen, mit denen Betroffenenrechte geltend gemacht werden, unterstützt. Damit ist allerdings keine Weiterleitungspflicht gemeint. Für den Regelfall wird man daher zur Wahrung der Betroffenenrechte eine ausdrückliche Klausel im Auftragsverarbeitervertrag aufnehmen, dass der Auftragsverarbeiter Anträge betroffener Personen an den Verantwortlichen weiterzuleiten hat. Das Auskunftsrecht kann in angemessenen Abständen wahrgenommen werden. Dies ist insb für die Frage relevant, ab wann von häufigen Wiederholungen im Sinne von exzessiven Anträgen gesprochen werden kann: Die Beurteilung der Angemessenheit wird auch davon abhängen, wie dynamisch der Datenbestand ist, und damit wie häufig Änderungen zu erwarten sind.

Das Bundesverwaltungsgericht sprach über das (Nicht-Bestehen) des Auskunftsrecht im Zusammenhang mit Papierakten aus (zB 28.05.2020, W274 2230370-1): Gemäß Art. 2 Abs. 1 DSGVO gilt diese für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Papierakten sind keine manuellen Datensysteme und unterliegen damit auch nicht dem datenschutzrechtlichen Auskunftsrecht. Als Dateisysteme zu qualifizieren sind jedoch Protokollbücher und Indexkarten, welche die Akten auffindbar machen. Akten von Behörden (Bescheid inklusive Spruch, Sachverhaltsfeststellungen, andere Teile der Bescheidbegründung sowie das diesem zugrunde liegende gesetzliche Ermittlungsverfahren) unterliegen keinem Auskunftsanspruch, auch wenn der entsprechende Text - wovon auszugehen ist - mithilfe automationsunterstützter Datenverarbeitung erstellt worden ist. Werturteile geben die subjektive Meinung des Erklärenden wieder und können

personenbezogene Daten anderer Personen enthalten. Auskünfte im Rahmen von Ermittlungs- oder Gerichtsverfahren sind im Wege der Akteneinsicht nach den einschlägigen Verfahrensbestimmungen einzuholen. Auf die von der belangten Behörde aufgeworfene Frage, wie weit das Recht auf Ausfolgung einer Datenkopie nach Art 15 Abs 3 DSGVO geht, ist mangels genereller Anwendbarkeit nicht einzugehen.

Die Datenschutzbehörde entschied, dass dem Auskunftsbegehren auch noch während des Verfahrens vor der Behörde – auch in mehreren Schritten – nachgekommen werden kann und damit die Beschwerde erledigt ist (24.04. 2020, 2020-0.219.620).

Right to Rectification

GDPR Provisions

The right to rectification means the right to obtain, without undue delay, the correction of personal data that is inaccurate. GDPR Art. 16.

Austria-Specific Additional Provisions

Pursuant to the Austrian DSG,[41] if personal data processed by automated means cannot be rectified immediately, because it can be rectified only at certain times for economic or technical reasons, processing of the personal data concerned shall be restricted until that time, with the effect as stipulated in GDPR Art. 18(2).

Right to Erasure or “Right to be Forgotten”

GDPR Provisions

The right of erasure means the right to obtain from the controller the erasure of personal data concerning the data subject without undue delay.[42] The data subject can request erasure when, among other things, the personal data is no longer necessary in relation to the purposes for which they were collected or processed, or the personal data have been unlawfully processed.

Austria-Specific Additional Provisions and Case Law

Pursuant to the Austrian DSG,[43] if personal data processed by automated means cannot be erased immediately, because it can be erased only at certain times for economic or technical reasons, processing of the personal data concerned shall be restricted until that time, with the effect as stipulated in GDPR Art. 18(2).

Das Bundesverwaltungsgericht entschied am 28.05.2020 zu W274 2230286-1: Gemäß Art. 17 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, allerdings ausschließlich unter den dort genannten Gründen. Ein Löschungsanspruch scheidet

[41]DSG Section 4(2).

[42]GDPR Art. 17.

[43]DSG Section 4(2).

daher insbesondere dann aus, wenn die Verarbeitung erforderlich ist, damit der Verantwortliche einer rechtlichen Verpflichtung nachkommen kann. Als ausdrückliche Rechtsgrundlage findet sich die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen nur in Art. 9 Abs. 2 lit. f DSGVO. Die Aufbewahrung des Löschungsantrags und sonstiger bezughabender Unterlagen wird der Verantwortliche auf diesen Ausnahmetatbestand stützen können, sofern diese Daten überhaupt vom Löschungsantrag erfasst sind.

Right to Restriction of Processing

GDPR Art. 18 grants data subjects the right to obtain from the controller restriction of processing of personal data in specific, limited circumstances. The grounds for restriction of the processing include: when the accuracy of the personal data is contested by the data subject, or where the controller no longer needs the personal data for the purposes of the processing but the data is required by the data subject for the establishment, exercise, or defense of legal claims.

Right to Portability

The right to portability is the right to receive personal data concerning the data subject that the data subject previously provided to the controller. The data must be provided in a structured and commonly used machine-readable format, and the data subject may require that the data be transmitted to another controller without hindrance.[44]

Right to Object

The right to object to certain forms of processing of personal data concerning the data subject that have been collected on specific legal grounds (such as controller's legitimate interest) is contained in GDPR Art. 21. This applies especially when the personal data is used for profiling or direct marketing purposes.

Right to Not Be Subject to Automated Decision Making, Including Profiling

The right to not be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning the data subject, including profiling is contained in GDPR Art. 22.

Controllers' Obligations to Data Subjects

Transparency

GDPR Art. 12 requires data controllers to provide the notices required under the GDPR in a concise, transparent, intelligible, and easily accessible form. The notices must use clear and plain language, in particular for any information addressed specifically to a child. The information must be provided in writing, or by other means, including by electronic means, or

[44]GDPR Art. 20.

may be provided orally at the data subject's request, provided that the identity of the data subject is proven by other means.

Content of Notices to Data Subjects

If the Data Subject Provided the Data

When personal data relating to a data subject is collected from the data subject, GDPR Art. 13 requires that the controller provide the data subject with all of the following information when the information is obtained:

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the data protection officer, where applicable;
- The purposes of the processing for which the personal data is intended, and the legal basis for the processing;
- If the processing is conducted for the legitimate interests pursued by the controller or by a third party, a description of the legitimate interest;
- The recipients or categories of recipients of the personal data, if any;
- Whether the controller intends to transfer personal data to a third country reference to the appropriate or suitable safeguards and how to a copy of them or where they have been made available.
- The retention period, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the controller access to, or rectification or erasure of personal data, or restriction of processing, right to object to processing, and right to data portability;
- Where the processing is based on consent, the existence of the right to withdraw consent at any time;
- The right to lodge a complaint with a supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement, or is necessary to enter into a contract, and whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data; and
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, and the significance and envisaged consequences for the data subject.

If the Data Subject Did Not Provide the Data

Where personal data have not been obtained from the data subject, GDPR Art. 14 requires the controller to provide the data subject with the following information within a reasonable period after obtaining the personal data, but at the latest 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 foreseen, at the latest when the personal data is first disclosed. The information to be provided includes:

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the data protection officer, where applicable;
- The purposes of the processing for which the personal data is intended and the legal basis for the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, that the controller intends to transfer personal data to a third country and reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;
- The retention period, or if that is not possible, the criteria used to determine that period;
- Whether the processing is conducted for the legitimate interests pursued by the controller or by a third party, a description of the legitimate interest;
- The existence of the right to request from the controller access to, or rectification or erasure of personal data, or restriction of processing, right to object to processing, and right to data portability;
- Where the processing is based on consent, the existence of the right to withdraw consent at any time;
- The right to lodge a complaint with a supervisory authority;
- From which source the personal data originate, and if applicable, whether it came from publicly accessible sources; and
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, and the significance and envisaged consequences for the data subject.

Other Obligations to Data Subjects

Data controllers have several obligations linked to the rights of a data subject in response to data subjects' requests. These include, for example, the obligation to facilitate the exercise of a data subject's rights (e.g., of information, access, erasure) (GDPR Arts. 15 to 17, Art. 20) and to respond to data subjects' objections to the processing of their data or requests to restrict the processing (GDPR Arts. 18, 21).

Obligations of Controllers

The GDPR contains several provisions focusing on the operations of the data controller.

Technical and Organization Measures to Ensure Compliance

GDPR Provisions

GDPR Art. 24(1) requires data controllers to implement appropriate technical and

organizational measures to ensure that the processing of personal data is performed in compliance with the GDPR. These measures must take into account the nature, scope, context, and purposes of the processing and the risks of varying likelihood and severity to the rights and freedoms of individuals. These measures must be reviewed and updated when necessary.

Austria-Specific Additional Provisions

Pursuant to the Austrian DSG,[45] the Controller, the Processors, and their employees, i.e. employees and persons in a quasi-employee relationship, shall ensure the confidentiality of personal data from data processing activities that have been entrusted or have become accessible to them solely due to their employment, without prejudice to other statutory obligations of confidentiality, unless a legitimate reason for the transmission of the data that have been entrusted or have become accessible to them exists ("Confidentiality of Data"). Employees may transmit personal data only if expressly ordered to do so by their employer.

Unless such an obligation of their employees already exists by law, the Controller and the Processor must contractually bind their employees to transmit personal data from data processing activities only on the basis of orders and to maintain the Confidentiality of Data even after the end of their employment with the Controller or Processor. The Controller and the Processor must inform the employees affected by these orders about the transmission orders applicable to them and about the consequences of a violation of data confidentiality.

Accountability

GDPR Arts. 5(2) and 24(1) require data controllers to demonstrate that their processing is performed in accordance with the GDPR.

Recordkeeping Requirements for Data Controllers

GDPR Art. 30 requires data controllers to keep records of their processing activities. The records must be in writing, including in electronic form. The controller must be prepared to make these records available to the data protection supervisory authority on request.

The record of processing activities must contain the following information:

- The name and contact details of the data controller, and, where applicable, those of any joint controller, data controller's representative, and data protection officer;
- The purposes of the processing;
- The categories of data subjects;
- The categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries;
- If applicable, transfers of personal data to a third country (including the name of the country);
- If applicable, documentation that establishes the legal basis for any cross-border transfers

[45] DSG Section 6.

and the related safeguards;

- When possible, the envisaged time limits for erasure of the different categories of data; and
- When possible, a general description of the technical and organizational security measures used to protect the personal data in the controller's custody.

Organizations with fewer than 250 employees are exempt from this recordkeeping requirement unless the processing:

- Is likely to result in a risk to the rights and freedoms of a data subject;
- Iis not occasional;
- Includes special categories of data (e.g., health or trade union membership data); or
- Is conducted on data relating to criminal convictions and offenses.

Data Protection by Design and by Default

GDPR Art. 25 requires data controllers to implement measures to ensure data protection by design and by default. These measures must take into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing, such as, for example, pseudonymization and data minimization. The measures must be adapted to face the varying risks to the rights and freedoms of natural persons posed by the processing.

Data Protection Impact Assessment (DPIA)

When a Data Protection Impact Assessment Is Required

GDPR Provisions.

When a proposed processing is likely to result in a high risk to the rights and freedoms of individuals, GDPR Art. 35 requires that the data controller assess the impact of the planned processing on the protection of personal data before commencing the processing.

GDPR Art. 35(3) identifies several situations where a DPIA is required:

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

Austria-Specific Additional Provisions.

The Austrian DSB has published information clarifying when a DPIA is required, and when

it is not. This information is provided in the form a "white list"[46] (where no DPIA necessary) and a "black list"[47] (where a DPIA required).

Content of the DPIA

GDPR Art. 35 defines the minimum content of a DPIA:

- Systematic description of the envisaged processing and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- Assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- Assessment of the risks to the rights and freedoms of data subjects; and
- Measures planned to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

In addition, when appropriate, the data controller must seek the views of data subjects on the intended processing.[48]

Prior Consultation with Supervisory Authority

When the DPIA indicates that the processing would result in a high risk for the data subjects in the absence of measures taken by the controller to mitigate the risk, GDPR Art. 36(2) requires the data controller to consult the supervisory authority before processing personal data unless the data controller elects to take specific measures to mitigate the risk.

If the supervisory authority determines that the intended processing would not comply with the GDPR, it must intervene within eight weeks following the request for consultation and give advice to the data controller. This period may be extended for a further six weeks, taking into account the complexity of the intended processing.

Cooperation with Supervisory Authority

GDPR Art. 31 requires a data controller and its representative, if any, to cooperate, on request, with the data protection supervisory authority in the performance of its tasks.

Responsibilities of Joint Controllers

The GDPR contains numerous provisions defining the responsibilities and obligations for controllers regarding the processing and protection of personal data. This responsibility may

[46]"*Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)*", https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.html (in German language).

[47]„*Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)*", https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_278/BGBLA_2018_II_278.html (in German language).

[48]GDPR Art. 35(9).

be vested in several data controllers. Under GDPR Art. 26, if several data controllers jointly determine the purposes and means of processing personal data, they are deemed “joint controllers.”

In this case, the joint data controllers must determine their respective responsibilities for compliance with the obligations under the GDPR, in particular with respect to their respective duties to provide the information referred to the data subject with respect to the processing of the personal data, the allocations of their respective responsibilities to the data subject. The essence of the arrangement must be made available to the data subject, and the data subjects may exercise their GDPR rights against each of the controllers.[49]

Data Processors

Recordkeeping Requirements

Data processors have recordkeeping obligations that are very similar to those of the data controllers. Under GDPR Art. 30(2), the record must contain the following information:

- The name and contact details of the data processor or subprocessors; of each data controller on behalf of which the data processor is acting; and, when applicable, of the data controller's or data processor's representative and the data protection officer, if any;
- The categories of processing carried out on behalf of each data controller;
- If applicable, a description of the transfers of data to a third country and, in some instances, the documentation of appropriate safeguards; and
- When possible, a description of the technical and organizational security measures being used.

GDPR Art. 30(5) exempts organizations with fewer than 250 employees from this recordkeeping requirement unless the data processing (1) is likely to result in a risk to the rights and freedoms of a data subject, (2) is not occasional, (3) includes special categories of data (e.g., health or trade union membership data), or (4) is conducted on data relating to criminal convictions and offenses.

Conditions for Processing Data by a Data Processor or Subprocessor

There are several significant conditions to the engagement of a data processor or subprocessor to process data on behalf of a data controller.

Sufficient Guarantees

First, if a data controller intends to entrust a third party with the processing of personal data, GDPR Art. 28 requires the controller to engage only data processors that provide sufficient guarantees to implement appropriate technical and organizational measures to ensure that the processing can meet the GDPR requirements and ensure the protection of data subjects' rights.

[49]GDPR Art. 26(3).

Written Data Processing Agreement Required

Second, GDPR Art. 28 requires that, when an entity engages a third to process personal in its behalf, the terms of the engagement be governed by a contract or other legal act that binds the data processor to the data controller. The contract must set out 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, and the obligations and rights of the data controller. It must require the data processor to:

- Process the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to a third country, unless otherwise required by applicable law to which the data processor is subject;
- Ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Take all appropriate security measures required by GDPR;
- Enlist another data processor only with the prior consent of the data controller and pursuant to a written contract with specified provisions;
- Assist the data controller by appropriate technical and organizational measures that take into account the nature of the processing in the fulfillment of the data controller's obligation to respond to a data subject's requests for access, erasure, or correction of his or her personal data;
- Assist the data controller in ensuring compliance with its security obligations;
- At the data controller's request, delete or return all the personal data to it after the end of the data processing services, and delete existing copies unless EU or Member State law requires storage of the data;
- Make available to the data controller all information necessary to demonstrate compliance with its obligations under GDPR, and allow for and contribute to audits and inspections conducted by the data controller or another auditor mandated by the data controller; and
- Immediately inform the data controller if, in his or her opinion, an instruction by the data controller breaches any provision of GDPR or any EU or Member State data protection provisions.

GDPR Art. 28(6) allows the contract between a data controller and a data processor to be based, in whole or in part, on standard contractual clauses.

In addition to the Art. 28 obligations, the data processing agreement must address the provisions of GDPR Arts. 44 to 50, which provide the rules regarding the transfer of data across borders and outside the EU/EEA region.

Controller's Prior Consent to the Use of Subprocessors

Third, GDPR Art. 28(2) prohibits a data processor from engaging another data processor without the prior written consent of the controller. The contract with the subprocessor must include the same data protection obligations as those that are required in a contract between the data controller and the data processor. If the subprocessor fails to fulfill its data protection obligations, the primary data processor remains fully liable to the data controller for the performance of that subprocessor's obligations.

No Further Processing Permitted

GDPR Art. 29 prohibits entities that are acting in a data processor and subprocessor capacity from processing personal data other than on instructions from the data controller, or from the applicable primary processor, unless required to do so by applicable law. The prohibition applies directly to the data processor in addition to the terms of the required contract. This clause makes the data processor directly liable under the GDPR, and its failure to comply would be directly enforceable by the applicable data protection authority.

Data Protection Officer

Entities Required to Appoint Data Protection Officer

GDPR Art. 37 requires data controllers and data processors other than public authorities to designate a data protection officer (DPO) when the core processing activities of the controller or the processor consist of

- Activities whose scope or purposes require regular and systematic monitoring of data subjects on a large scale, or
- Processing on a large-scale data that are part of the “special categories of data” (e.g., data pertaining to health or race) or data relating to criminal convictions and offenses.

The controller or processor that has appointed a DPO must publish the DPO's contact details and communicate these details to the supervisory authority.[50]

A group of entities (e.g., the different companies in a corporate group) may appoint a single data protection officer, provided that the DPO is easily accessible from each establishment.

Qualifications of a Data Protection Officer

GDPR Art. 37 identifies the basic requirements for engaging a DPO. The person should be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices, and the ability to fulfill the tasks normally assigned a DPO. The DPO may be a staff member of the data controller or data processor. The function of the DPO may be outsourced to a third party on the basis of a contract for services.

Position of Data Protection Officer

GDPR Art. 38 describes the framework for the position of DPO.

The DPO must report directly to highest management levels of the controller or processor, and the DPO must not receive instructions regarding the exercise of his/her task. The DPO may not be dismissed for performing his/her tasks.[51]

The data controller or processor must ensure that its DPO is involved in all issues that relate to the protection of personal data. It must provide the DPO with resources necessary to carry out the DPO's tasks, access to personal data and processing operations, and the means to maintain their expert knowledge.

[50]GDPR Art. 37(7).

[51]GDPR Art. 38(3).

Tasks of Data Protection Officer

GDPR Art. 39 specifies the responsibilities of data protection officers. They include, for example:

- Inform and advise the entity and the employees who carry out processing of their obligations under GDPR;
- Monitor compliance with the GDPR and the applicable laws and with the policies of the controller or processor regarding personal data protection;
- Advise, when requested, on the conduct of a data protection impact assessment and monitor the performance of the assessment;
- Cooperate with the applicable supervisory authority; and
- Act as contact point for the applicable supervisory authority on issues related to the processing of personal data, including prior consultation.

Additional Austrian Requirements for Data Protection Officers

The Austrian DSG provides the following special provisions on DPOs:[52]

Confidentiality

Under Section 5 of the DSG, the DPO and the persons working for the DPO have an obligation of confidentiality when fulfilling their duties. This obligation applies in particular to protecting to the identity of data subjects who applied to the DPO, and to circumstances that allow identification of these persons, unless the data subject has expressly granted a release from confidentiality.

The DPO and the persons working for the DPO may exclusively use information made available to fulfil their duties and are bound by confidentiality even after the end of their activities.

If, during his or her activities, a DPO obtains knowledge of data in respect of which a person employed with an entity that is subject to the DPO's supervision, the DPO has a statutory right to refuse to give evidence, the DPO and the persons working for the DPO also have such right to the extent to which the person who has the right to refuse to give evidence exercised that right.

The files and other documents of the DPO are protected from seizure and confiscation to the extent of the right of the DPO to refuse to give evidence.

Public Sector DPO

In the public sector, one or several DPO must be appointed in the sphere of responsibilities of each federal ministry, taking into account the type and scope of data processing activities and depending on the facilities of the relevant federal ministry. These DPO's will be employed by the relevant federal ministry or the relevant subordinate office or other entity.

[52]DSG Section 5.

Public-Sector DPO's are not bound by any instructions when exercising their duties. The highest governing bodies or officers have the right to obtain information on matters to be dealt with from a Public-Sector DPO. The DPO must provide information only insofar as the independence of the DPO as described in GDPR Art. 38(3) is not impaired by doing so.

The Austrian law also requires that Public-Sector DPO's regularly exchange information, in particular with regard to ensuring uniform data protection standards.

Security of Personal Data

Technical and Organizational Measures Required

GDPR Provisions

Both controllers and processors are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of data processing. The measures must take into account the nature, scope, context, and purposes of the processing, the risk of varying likelihood and severity to the rights and freedoms of individuals, the state of the art, and the costs of implementation.[53] According to GDPR Art. 32, these measures must include, as appropriate:

- Pseudonymization;
- Encryption;
- Ensuring the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data;
- Ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Austria-Specific Additional Provisions

In Austria, at a (more or less) technical level, the Federal Act on Data Security Measures when using Personal Electronic Health Data 2012 ("*Gesundheitstelematikgesetz–GTelG 2012"*) and the Regulation on Data Security Measures when using Personal Electronic Health Data ("*Gesundheitstelematikverordnung*") deal with the security measures of the processing of personal health data. Objectives of those regulations are to foster and extend data security when using electronic health data in directed or undirected communication by setting up uniform federal minimum standards and avoiding abuse of data; to provide and broaden the information basis necessary for the steering and development of e-health in Austria; as well as to create uniform rules for undirected communication of electronic health data. The Austrian Electronic Health Record—EHR ("*Elektronischer Gesundheitsakt—ELGA*") was established by the GTelG 2012.

The DSG[54] stipulates special provisions on the processing for archiving purposes in the

[53]GDPR Art 32.

[54]DSG Section 7.

public interest, scientific or historical research purposes or statistical purposes, including special categories of data. Furthermore, the Austrian Data Protection Adaptation Act for Science and Research 2018 ("*Datenschutzanpassungsgesetz Wissenschaft und Forschung 2018" - FOG*) provides a specific data protection regime in the field of science and research, including special categories of data, especially health data:

Für Verarbeitungen sind dabei insbesondere folgende angemessene Maßnahmen, wie sie insbesondere in Art. 9 Abs. 2 Buchstabe j sowie Art. 89 Abs. 1 DSGVO vorgesehen sind, einzuhalten:

- Zugriffe auf personenbezogene Daten sind lückenlos zu protokollieren;
- Das Datengeheimnis (§ 6 DSG) ist einzuhalten;
- Verantwortliche haben
  - im Internet öffentlich einsehbar auf die Inanspruchnahme dieser Rechtsgrundlage hinzuweisen,
  - bei Ausstattung ihrer Daten mit bereichsspezifischen Personenkennzeichen die Namensangaben jedenfalls zu löschen,
  - vor Heranziehung von Registern jedenfalls einen Datenschutzbeauftragten (Art. 37 DSGVO) zu bestellen,
  - die Aufgabenverteilung bei der Verarbeitung der Daten zwischen den Organisationseinheiten und zwischen den Mitarbeiterinnen und Mitarbeitern ausdrücklich festzulegen,
  - die Verarbeitung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
  - (zumindest) die im Gesetz festgelegten technischen und organisatorischen Maßnahmen einzusetzen;
  - ihrem Antrag auf Bereitstellung von Daten an die Register eine von der oder dem Verfügungsbefugten über die Datenbestände aus denen die personenbezogenen Daten ermittelt werden sollen, unterfertigte Erklärung anzuschließen, dass sie oder er dem Verantwortlichen die Datenbestände für die Untersuchung zur Verfügung stellt, wobei anstelle dieser Erklärung auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 EO) vorgelegt werden kann,
- bei Übermittlung von Namensangaben sind diese nach Erreichung der Zwecke gemäß Art. 89 Abs. 1 DSGVO zu löschen.
- Die Veröffentlichung von bereichsspezifischen Personenkennzeichen darf unter keinen Umständen erfolgen.

Zur Erleichterung der Identifikation im Tätigkeitsbereich „Forschung" (BF-FO) sind die §§ 14 und 15 E-GovG im privaten Bereich nicht anzuwenden. Stattdessen sind die Bestimmungen des E-GovG, die für Verantwortliche des öffentlichen Bereichs gelten, wie insbesondere die §§ 8 bis 13 E-GovG, anzuwenden.

Wissenschaftliche Einrichtungen dürfen, insbesondere auf Grundlage des Art. 9 Abs. 2 Buchstabe g, i und j DSGVO, somit

- sämtliche personenbezogene Daten jedenfalls verarbeiten, insbesondere im Rahmen von

Big Data, personalisierter Medizin, biomedizinischer Forschung, Biobanken und der Übermittlung an andere wissenschaftliche Einrichtungen und Auftragsverarbeiter, wenn

a) anstelle des Namens, bereichsspezifische Personenkennzeichen für den Tätigkeitsbereich „Forschung“ (bPK-BF-FO) oder andere eindeutige Identifikatoren zur Zuordnung herangezogen werden oder

b) die Verarbeitung in pseudonymisierter Form (Art. 4 Nr. 5 DSGVO) erfolgt oder

c) Veröffentlichungen nicht oder nur in anonymisierter oder pseudonymisierter Form oder ohne Namen, Adressen oder Foto erfolgen oder

d) die Verarbeitung ausschließlich zum Zweck der Anonymisierung oder Pseudonymisierung erfolgt und keine Offenlegung direkt personenbezogener Daten an Dritte (Art. 4 Nr. 10 DSGVO) damit verbunden ist,

– die Ausstattung ihrer Daten mit bereichsspezifischen Personenkennzeichen für den Tätigkeitsbereich „Forschung“ (bPK-BF-FO) sowie von verschlüsselten bPK gemäß § 13 Abs. 2 E-GovG innerhalb der in Art. 12 Abs. 3 DSGVO genannten Frist von der Stammzahlenregisterbehörde verlangen, wenn

a) die Antragstellerin oder der Antragsteller eine wissenschaftliche Einrichtung ist,

b) die Kosten für die Ausstattung mit bereichsspezifischen Personenkennzeichen ersetzt werden und

c) die Antragstellerin oder der Antragsteller zumindest Vorname, Nachname und Geburtsdatum für jeden auszustattenden Datensatz bereitstellt

– von Verantwortlichen, die bundesgesetzlich vorgesehene Register – mit Ausnahme der in den Bereichen der Gerichtsbarkeit sowie der Rechtsanwälte und Notare im Rahmen des jeweiligen gesetzlichen Wirkungsbereichs geführten Register und des Strafregisters – führen, sowie im Falle von ELGA von der ELGA-Ombudsstelle, die Bereitstellung von Daten innerhalb der in Art. 12 Abs. 3 DSGVO genannten Frist aus diesen Registern in elektronischer Form verlangen, wobei Namensangaben durch bereichsspezifische Personenkennzeichen „Forschung“ (bPK-BF-FO) zu ersetzen sind, es sei denn die Namensangaben sind zur Erreichung von Zwecken gemäß Art. 89 Abs. 1 DSGVO erforderlich, wenn

a) die Verarbeitung ausschließlich für Zwecke der Lebens- und Sozialwissenschaften erfolgt,

b) das Register in einer Verordnung gemäß § 38b angeführt ist,

c) die Antragstellerin oder der Antragsteller eine wissenschaftliche Einrichtung ist,

d) die Kosten für die Bereitstellung der Daten ersetzt werden und

e) falls ein Abgleich mit vorhandenen Daten beantragt wird, beim Antrag auf Bereitstellung der Daten die entsprechenden bPK gemäß § 13 Abs. 2 E-GovG der betroffenen Personen zur Verfügung gestellt werden.

Die Verarbeitung von Daten ist gemäß Art. 9 Abs. 2 Buchstabe j DSGVO zulässig, wenn die betroffene Person freiwillig, in informierter Weise und unmissverständlich ihren Willen in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung bekundet, mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden zu sein, wobei die Angabe eines Zweckes durch die Angabe eines Forschungsbereiches oder

mehrerer Forschungsbereiche oder von Forschungsprojekten oder von Teilen von Forschungsprojekten erfolgen darf („broad consent“).

Hinsichtlich der Weiterverarbeitung gemäß Art. 5 Abs. 1 Buchstabe b DSGVO zu Zwecken gemäß Art. 89 Abs. 1 DSGVO stellen diese keine unzulässigen Zwecke im Sinne des § 62 Abs. 1 Z 2 DSG dar.

Gemäß Art. 5 Abs. 1 Buchstabe e DSGVO dürfen personenbezogene Daten für Zwecke gemäß Art. 89 Abs. 1 DSGVO unbeschränkt gespeichert und gegebenenfalls sonst verarbeitet werden, soweit gesetzlich keine zeitlichen Begrenzungen vorgesehen sind.

Die folgenden Rechte finden insoweit keine Anwendung, als dadurch die Erreichung von Zwecken gemäß Art. 89 Abs. 1 DSGVO voraussichtlich unmöglich gemacht oder ernsthaft beeinträchtigt wird:

- Auskunftsrecht der betroffenen Person (Art. 15 DSGVO),
- Recht auf Berichtigung (Art. 16 DSGVO),
- Recht auf Löschung bzw. Recht auf Vergessenwerden (Art. 17 DSGVO),
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO),
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO) sowie
- Widerspruchsrecht (Art. 21 DSGVO).

Auf Grundlage des Art. 9 Abs. 2 Buchstabe j DSGVO ist die Einholung einer Genehmigung der Datenschutzbehörde gemäß § 7 Abs. 2 Z 3 DSG nicht erforderlich, wenn die Verarbeitung in Übereinstimmung mit dem FOG erfolgt.

Der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten als auch die Auswertung von mittels Bildaufnahmen gewonnen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium für Zwecke gemäß Art. 89 Abs. 1 DSGVO ist zulässig, vorausgesetzt

- die Verarbeitung erfolgt durch wissenschaftliche Einrichtungen und
- durch die Verarbeitung erfolgt keine Veröffentlichung personenbezogener Daten.

Wissenschaftliche Einrichtungen dürfen Forschungsmaterial für Zwecke gemäß Art. 89 Abs. 1 DSGVO insbesondere sammeln, archivieren und systematisch erfassen und dazu sämtliche Daten verarbeiten, die erforderlich sind, um einen optimalen Zugang zu Daten und Forschungsmaterial für Zwecke gemäß Art. 89 Abs. 1 DSGVO („Repositories“) zu gewährleisten, wie insbesondere:

- Namensangaben,
- Personenmerkmale, sowie insbesondere: Zugehörigkeit zu einer sozialen, ethnischen oder kulturellen Gruppe; soziale Stellung; Beruf; Sprachkenntnisse und sonstige, besondere Kenntnisse; vorherige Angaben hinsichtlich der Vorfahren; Personenkennung, insbesondere durch bereichsspezifisches Personenkennzeichen des Tätigkeitsbereichs „Bildung und Forschung“;
- soweit verfügbar, Angaben zu sonstigen Betroffenen gemäß § 6 Abs. 4 E-GovG, die in Beziehung zu den natürlichen Personen stehen, deren Daten verarbeitet werden sollen: Bezeichnung; Rechtsform; elektronische Kennung gemäß § 6 Abs. 3 E-GovG; Angaben

zur Beziehung zwischen den sonstigen Betroffenen und den natürlichen Personen, deren Daten verarbeitet werden sollen; Gründungsdatum; Adress- und Kontaktdaten;

- sonstige Daten, die für die Archivierung und Klassifikation erforderlich sind, wie etwa Fundortdaten oder Angaben zu Personen, die das Forschungsmaterial zur Verfügung gestellt haben, sowie
- weitere Angaben, wie insbesondere: politische Hintergrundinformationen; religiöse Hintergrundinformationen; rechtliche Hintergrundinformationen; traditionelle Hintergrundinformationen; Hintergrundinformationen betreffend die Gesundheit, Gesundheitsdaten oder genetische Daten oder andere gruppenspezifische Hintergrundinformationen.

Wissenschaftliche Einrichtungen, die Verantwortliche der Repositories sind, dürfen anderen wissenschaftlichen Einrichtungen direkt personenbezogene Daten bereitstellen, wenn

- sie die anderen wissenschaftlichen Einrichtungen über deren datenschutzrechtlichen Pflichten nachweislich aufgeklärt haben,
- sie Vorkehrungen dafür getroffen haben, dass die anderen wissenschaftlichen Einrichtungen ihre Pflichten einhalten, und
- eine von einer vertretungsbefugten Person der anderen wissenschaftlichen Einrichtung unterfertigte Erklärung vorliegt, dass gegenüber der anderen wissenschaftlichen Einrichtung in den letzten drei Jahren keine Untersagung gemäß § 22 Abs. 4 DSG erfolgte und keine Maßnahme gemäß Art. 58 Abs. 2 Buchstaben f bis j DSGVO gesetzt wurde.

Daten und Forschungsmaterial, die als Grundlage für Tätigkeiten zu Zwecken gemäß Art. 89 Abs. 1 DSGVO verarbeitet wurden („Rohdaten“), dürfen ab Veröffentlichung der Ergebnisse dieser Tätigkeiten

- zum Nachweis der Einhaltung guter wissenschaftlicher Praxis mindestens 10 Jahre sowie
- zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen bis zu 30 Jahre

gespeichert und gegebenenfalls sonst verarbeitet werden.

Verarbeitungen im Rahmen von biologischen Proben- und Datensammlungen aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, stellen zulässige Verarbeitungen im Sinne des Art. 9 Abs. 2 Buchstaben h, i und j DSGVO dar. Die Verantwortlichen haben jedenfalls die folgenden, angemessenen und spezifischen Maßnahmen vorzusehen:

- die schnellstmögliche Pseudonymisierung, wenn dennoch die Zwecke der Verarbeitungen erfüllt werden können, sowie
- die Einhaltung der gemäß Art. 32 DSGVO erforderlichen Datensicherheitsmaßnahmen.

Für Zwecke der Lehre, insbesondere das Verfassen schriftlicher Seminar- und Prüfungsarbeiten, Bachelorarbeiten sowie wissenschaftlicher und künstlerischer Arbeiten durch Studierende, dürfen sämtliche personenbezogene Daten verarbeitet werden, wenn sichergestellt ist, dass – außer zulässigen Verarbeitungen – keine Übermittlung an Empfängerinnen oder Empfänger zu anderen Zwecken als gemäß Art. 89 Abs. 1 DSGVO erfolgt.

Für Zwecke der medizinischen Forschung und sterbefallbezogener Analysen darf die Bundesanstalt Statistik Österreich wissenschaftlichen Einrichtungen nach Vereinbarung der konkreten Anwendungsbereiche und eines angemessenen Kostenersatzes das Sterbedatum und die Todesursache von Betroffenen übermitteln. Die wissenschaftlichen Einrichtungen und deren Angehörige unterliegen hinsichtlich dieser Daten der Geheimhaltungspflicht gemäß § 17 Abs. 3 des Bundesstatistikgesetzes 2000 und dürfen diese Daten ausschließlich für wissenschaftliche Zwecke verwenden.

An Medizinischen Universitäten bzw. Universitäten, an denen eine Medizinische Fakultät eingerichtet ist, ist vor Übermittlung gemäß Abs. 6 die Ethikkommission gemäß § 30 UG zu befassen. An anderen wissenschaftlichen Einrichtungen (§ 2b Z 12) ist – sofern eingerichtet – eine Ethikkommission gemäß § 8c KAKuG oder eine vergleichbare Ethikkommission zu befassen."

Ungeachtet allfälliger patentrechtlicher Bestimmungen ist die Verarbeitung für Technologietransfer zulässig, wenn

- diese Verarbeitung erforderlich ist, um die Funktionalität der zu transferierenden Technologie zu erhalten, und
- insbesondere durch Technikgestaltung gemäß Art. 25 DSGVO sichergestellt ist, dass Dritte (Art. 4 Nr. 10 DSGVO) keine tatsächliche Kenntnis der übermittelten Daten erlangen.

Unter diesen Voraussetzungen finden die Pflichten und Rechte gemäß den Art. 12 bis 22 und Art. 34 DSGVO sowie Art. 5 DSGVO, insofern dessen Bestimmungen den in den Art. 12 bis 22 DSGVO vorgesehenen Rechten und Pflichten entsprechen, keine Anwendung auf Technologietransfer.

Werden im Rahmen von Open-Science- und Citizen-Science-Projekten eigene personenbezogene Daten freiwillig zur Verfügung gestellt, ist ihre Verarbeitung für die zu Beginn des Projekts ausdrücklich kommunizierte Art, Umfang und Dauer zulässig. Die Löschung ist nur zulässig, wenn dadurch die Projektziele und die methodischen, insbesondere statistischen, Anforderungen an wissenschaftliches Arbeiten nicht beeinträchtigt werden.

Werden im Rahmen von Open-Science- und Citizen-Science-Projekten personenbezogene Daten Dritter (Art. 4 Nr. 10 DSGVO) zur Verfügung gestellt, ist ihre Verarbeitung für die zu Beginn des Projekts ausdrücklich kommunizierte Art, Umfang und Dauer jedenfalls zulässig, wenn die Daten auf Beobachtungen oder Messungen im öffentlichen Raum beruhen oder die Daten im Sinne des Art. 4 Nr. 5 DSGVO pseudonymisiert werden.

Weiters bestehen Sonderbestimmungen hinsichtlich der Internationalität von Verarbeitungen gemäß Art. 89 DSGVO und zum Rechtsschutz.

Breach of Security

GDPR Art. 4(12) defines "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Notification of the Supervisory Authority

GDPR Provisions.

If there is a personal data breach, the data controller must, without undue delay, and when feasible not later than 72 hours after having become aware of it, give notice of the breach to the competent supervisory authority, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.[55] If notification is not made within 72 hours, the data controller must provide to the supervisory authority a reasonable justification explaining the reason for the delay.

The notification to the supervisory authority must provide at least the following information:

- Description of the nature of the breach, including when possible the categories and approximate numbers of data subjects and data records concerned;
- Name and contact details of the data protection officer or other contact point where more information can be obtained;
- Description of the likely consequences of the personal data breach; and
- Description of the measures taken or proposed to be taken by the data controller to address the breach, including, when appropriate, to mitigate its possible adverse effects.

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

The data controller must document a personal data breach, including the facts surrounding the breach, its effects, and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with the controller's obligation under the applicable provisions of the GDPR.

Austria-Specific Additional Provisions.

The Austrian DSB provides special forms for the notification of data breaches (also in the English language).[56]

Notification of the Data Subjects

GDPR Art. 34(1) requires the data controller that has suffered a personal data breach to notify the data subjects “without undue delay” when the personal data breach is likely to “result in a high risk to the rights and freedoms of individuals affected.”

The communication to the data subject must describe in clear and plain language the nature of the personal data breach and contain at least the same information as that which has been provided to the Supervisory authority:

- Description of the nature of the breach, including when possible the categories and approximate numbers of data subjects and data records concerned;
- Name and contact details of the data protection officer or other contact point where more information can be obtained;

[55] GDPR Art. 33.

[56] https://www.dsb.gv.at/documents/22758/1188945/Meldung+von+Verletzungen+des+Schutzes+personenbezogener+Daten+gem%c3%a4%c3%9f+Art.+33+DSGVO+Notification+of+a+personal+data+breach+(Art.+33+GDPR)+.pdf/61fc399f-f77f-4b61-b994-e4db7a7656b5.

- Description of the likely consequences of the personal data breach; and
- Description of the measures taken or proposed to be taken by the data controller to address the breach, including, when appropriate, to mitigate its possible adverse effects.

The communication to the data subject is not required if any of the following conditions are met:

- The controller has implemented appropriate technical and organizational 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 authorized to access it, such as encryption;
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize
- 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.

In addition, 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 or may decide that any of the conditions referred to above are met.

Breach Affecting a Data Processor

If the breach affects a data processor, it must notify the data controller without undue delay after becoming aware of a personal data breach.[57]

Crossborder Data Transfers

GDPR Arts. 44 to 49 define the rules applicable to crossborder data transfers. Any transfer of personal data to a third country for processing may take place only if the data controller and data processor comply with rules regarding the transfer of personal data to third countries as set forth in GDPR Arts. 44 to 49.

Transfers on the Basis of an Adequacy Decision

Transfer of personal data to a third country may take place when the EU Commission has determined that the receiving country ensures an adequate level of protection.[58] GDPR Arts. 45(4) and 45(9) allow for the survival of the adequacy decisions adopted by the EU Commission on the basis of Art. 25(6) of Directive 95/46/EC until these decisions are amended, replaced, or repealed by a Commission decision.

Currently, the countries outside the EEA that have been recognized as providing adequate protection include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay, as well as the EU-US Privacy Shield

[57]GDPR Art. 33(2).

[58]GDPR Art. 45(1).

Framework.[59] Adequacy talks are ongoing with South Korea.

Transfers to a third country that does not meet the conditions above are not possible unless an exception or a derogation applies. GDPR Arts. 45, 46, and 49 provide the rules that apply when the data is to be transferred and/or processed in a country for which the EU Commission has not made a determination that the country offers adequate protection.

Transfers by Way of Appropriate Safeguards

General Rules

In the absence of an adequacy decision as discussed above, a data controller or data processor may transfer personal data to a third country only if the data controller or data processor has provided appropriate safeguards and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.[60]

The "appropriate safeguards" set forth in GDPR Art. 46(1) may be provided, without a specific authorization from a supervisory authority, by:

- A legally binding and enforceable instrument between public authorities or bodies;
- Binding Corporate Rules;
- Standard data protection clauses adopted by the EU Commission;
- Standard data protection clauses adopted by a supervisory authority and approved by the EU Commission;
- An approved code of conduct with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including those that pertain to data subjects' rights; or
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including those regarding data subjects' rights.

Binding Corporate Rules

GDPR Art. 47 establishes the legitimacy of the Binding Corporate Rules (BCR) as a means to show adequacy in relations to crossborder data transfer. GDPR Art. 47 also establishes the rule regarding the content and approval of BCR.

To be eligible for approval by the competent data supervisory authority, proposed BCR must meet two sets of criteria. First, under GDPR Art. 47(1), they must

- Be legally binding and apply to and are enforced by every member of a group of entities or groups of enterprises engaged in a joint economic activity, including their employees;
- Expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

[59]Current list available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[60]GDPR Art. 46(1).

- Fulfill the requirements set forth in GDPR Art. 47(2).

Second, the BCR must contain the content specified in GDPR Art. 47(2). To meet this obligation, BCR shall specify at least:

- The structure and contact details of the group of enterprises engaged in a joint economic activity and of each of its members;
- The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- Their legally binding nature, both internally and externally;
- The application of the general data protection principles, in particular purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements for onward transfers to bodies not bound by the binding corporate rules;
- The rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
- The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union;
- How the information on the binding corporate rules is provided to the data subjects;
- The tasks of any data protection officer or any other person or entity in charge of the monitoring compliance with the BCR within the group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
- The complaint procedures;
- The mechanisms within the group of enterprises for ensuring the verification of compliance with the BCR, including data protection audits and methods for ensuring corrective actions to protect the rights of the data subject;
- The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
- The mechanisms for cooperation with the supervisory authority to ensure compliance by any member of the group of enterprises, in particular by making available to the supervisory authority the results of verifications of the measures;
- The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group enterprises is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the BCR; and
- The appropriate data protection training to personnel having permanent or regular access to personal data.

Standard Contractual Clauses

GDPR Art. 46(2) also allows businesses intending to receive data from an EU or EEA Member State to enter into a contract with the data exporter in which the two entities commit to provide adequate safeguards for the data. Several documents are available for different situations. They were drafted and approved by the European Commission while Directive 95/46/EC was in effected, and it is likely that they may be replaced in the long term by other documents.

[Controller-Controller Transfers.

For transfers from data controller to data controller, two documents are available: one published in 2001 (see EU Commission Decision 2001/497/EC (June 15, 2001)) and the other in 2004 (see EU Commission Decision 2004/915/EC (Dec. 27, 2004)).

Controller-Processor Transfers.

For transfers from data controller to data processor, the current version of the form agreement to be used is found in Commission Decision 2010/87/EU. This document supersedes a preexisting document, which was published in 2004.

Derogations for Specific Situations

GDPR Provisions

In the absence of an adequacy decision or appropriate safeguards, such as BCRs or Standard Contractual Clauses, GDPR Art. 49 allows transfers of personal data in a number of specific circumstances. These circumstances include:

- The data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers for the data subject 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 precontractual 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;
- The transfer is necessary for the establishment, exercise, or defense of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other persons when the data subject is physically or legally incapable of giving consent; or
- The transfer is made from a register that, under EU or Member State law, is intended to provide information to the public and that is open to consultation by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by the EU or Member State law for consultation are fulfilled in the particular case.

  In those circumstances, the transfer may occur only if:

- It is not repetitive, concerns only a limited number of data subjects, and is necessary for the purposes of compelling legitimate interests pursued by the data controller that 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, based on this assessment, it adduced suitable safeguards with respect to the protection of personal data.

The data controller must inform the competent supervisory authority and the concerned data subjects about the proposed transfer and the compelling legitimate interests pursued by the data controller.

Austria-Specific Additional Provisions

The Austrian DSG stipulates that administrative decisions that permit the transfer of data abroad shall be revoked once the legal or factual prerequisites for the issue of the permit no longer apply.[61]

Transfers or Disclosures in the Context of Litigation

GDPR Provisions

Special rules apply to transfer of data in connection with litigation. Under GDPR Art. 48, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a data controller or data processor to transfer or disclose personal data may only be recognized or enforceable if it is based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer.

In addition, a number of Member States have adopted “blocking statutes” that prohibit certain transfers of data—personal or not—in connection with litigation. These blocking statutes were enacted to protect valuable commercial information from being transferred abroad, out of a concern that the U.S. rules of procedure might give U.S. litigants the opportunity to have access to valuable confidential information under the guise of discovery requests.

Austria-Specific Additional Provisions

In this context, it might be useful to take into account that the Austrian DSG[62] stipulates that the processing of personal data on acts or omissions punishable by courts or administrative authorities, in particular concerning suspected criminal offences, as well as data on criminal convictions and precautionary measures involving the deprivation of liberty, is permitted if the requirements of the GDPR are met and if (i) an explicit legal authorization or obligation to process such data exists; or (ii) the legitimacy of the processing of such data is otherwise based on statutory duties of diligence, or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party pursuant to GDPR Art. 6(1)(f), and the manner in which the data is processed safeguards the interests of the data subject according the GDPR and the DSG.

[61]DSG Section 25(4).

[62]DSG Section 4(3).

Codes of Conduct and Certification Mechanisms

GDPR Arts. 40 to 43 allow for the creation of codes of conducts and certification bodies intended to help entities subject to the GDPR demonstrate their compliance with the law. Codes of conduct will provide a structure that entities subject to the Regulation could follow in order to self-certify their adherence to that code of conduct. Certification bodies would attest of the compliance by auditing applicants and verifying that the applicant practices conform to the required rules. Numerous sections of the GDPR make reference to compliance with a Code of Conduct or a certificate from a certification body as a means to demonstrate compliance with relevant provisions of the GDPR.

Codes of Conduct

GDPR Provisions

GDPR Art. 40 prompts Member States, supervisory authorities, as well as the EDPB and EU Commission to encourage the creation of codes of conduct to assist in the proper implementation of the GDPR in specific sectors, or by specific categories of businesses, such as micro, small and medium-sized enterprises.

The codes of conduct are to be prepared by associations and other bodies representing categories of controllers or processors, and are to address specific aspects of the GDPR, such as those concerning fair and transparent processing; legitimate interest; collection of personal data; pseudonymization of personal data; information provided to the public and to data subjects; the exercise of the rights of data subjects; the handling of children personal information; measures and procedures that controllers and processors must take to show their compliance with the GDPR, security obligations; data breach notification obligations; cross border data transfers or the handling of disputes.

Codes of conduct may be specific to a Member State or may relate to processing activities in several Member States. After review by the relevant supervisory authority or authorities, the EU Commission may decide that the approved code of conduct has general validity within the entire Union.

Austria-Specific Additional Provisions

The Austrian DSB has issued Guidelines on the accreditation of Codes of Conducts and has already confirmed some.[63] Furthermore, the DSB issued a Regulation on the Requirements of a Monitoring Body on Codes of Conducts.[64]

Certification

Member States, supervisory authorities, the EDPB, and the EU Commission may also, as provided in GDPR Art. 43, encourage the establishment of data protection certification mechanisms and data protection seals and marks, through which controllers and processors

[63]https://www.dsb.gv.at/genehmigung-von-verhaltensregeln (in German language).

[64]"*Verordnung der Datenschutzbehörde über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellenakkreditierungs-Verordnung – ÜstAkk-V)*", https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2019_II_264/BGBLA_2019_II_264.html (in the German language).

can demonstrate their compliance with the Regulation. The certification will be issued by certification bodies that have been accredited by the competent supervisory authority or a national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the competent supervisory authority.

Austrian Framework

Pursuant to the DSG,[65] the DSB is the only national accreditation body pursuant to GDPR Art. 43(1)(a). The DSB issued a Regulation on Accreditation.

Supervisory Authority

Overview

GDPR Provisions

Article 51 of the GDPR requires each Member State to set up one or more independent public authorities to be responsible for monitoring the application of GDPR, protecting the fundamental rights and freedoms of natural persons in relation to the processing of their personal data, and facilitating the free flow of personal data within the EU. Each supervisory authority is expected to contribute to the consistent application of the GDPR throughout the EU.

Austria-Specific Additional Provisions

The Austrian DSG[66] establishes the *Österreichische Datenschutzbehörde* (DSB), which acts as the country's data protection authority. Pursuant to the Austrian DSG, the DSB is established as a national supervisory authority as provided for in GDPR Art. 51.

The DSB is managed by its head. If the head is absent, his or her deputy is responsible for managing the DSB. The rules regarding the head of the DSB also apply to the deputy.

The DSB has an independent status and acts as an authority supervising staff and as a human resource department. During his or her term of office, the head must not exercise any function that (i) could cast doubt on the independent exercise of his or her office or impartiality, (ii) prevents him or her from performing their professional duties, or (iii) puts essential official interests at risk.

The head is required to report functions that he or she exercises alongside his or her office as the head of the DSB to the Federal Chancellor without delay. The Federal Chancellor can request information from the head of the DSB on matters to be dealt with by the Authority. The head of the DSB has to meet this request only insofar as it does not impair the complete independence of the supervisory authority as described in GDPR Art. 52.

The DSB must prepare an activity report complying with GDPR Art. 59 by March 31 of every year and submit it to the Federal Chancellor. The Federal Chancellor must submit the report to the Federal Government, the National Council, and the Federal Council. The DSB

[65]DSG Section 21(3).

[66]DSG Sections 18 to 23 and 31 to 35.

must make the report accessible to the public, the European Commission, the European Data Protection Board, and the Data Protection Council.

Decisions made by the DSB that are of fundamental importance to the public must be published by the DSB in an appropriate manner while respecting official secrecy rules.[67]

Tasks of Supervisory Authorities

GDPR Provisions

GDPR Art. 57 identifies the tasks of supervisory authorities. Among these tasks, the following are especially important for businesses:

- Monitoring and enforcing the application of the GDPR;
- Promoting the awareness of controllers and processor of their obligations under GDPR;
- Informing data subjects concerning their rights;
- Handling complaints lodged by data subjects or entities, investigating the subject matter of a complaint, and informing the complainant of the progress and the outcome of the investigation;
- Cooperating with, and providing mutual assistance to, other supervisory authorities to ensure the consistency of application and enforcement of GDPR;
- Conducting investigations on the application of GDPR;
- Adopting standard contractual clauses;
- Establishing and maintaining a list of requirements for a data protection impact assessment;
- Approving Binding Corporate Rules;
- Contributing to the activities of the European Data Protection Board; and
- Keeping internal records of infringement of GDPR and of measures taken.

Austria-Specific Additional Provisions

The DSB advises the committees of the National Council, the Federal Council, the Federal government, and the State governments on legislative and administrative measures upon their request.[68] The DSB shall be heard before federal acts as well as regulations within the enforcement jurisdiction of the federal state are enacted that directly concern questions of data protection.

The DSB shall make public the lists pursuant to GDPR Art. 35(4) and (5) (Data Protection Impact Assessment (DPIA)) by way of an ordinance published in the Federal Law Gazette.

[67] *See* https://www.ris.bka.gv.at/Dsk/ (only in German language).

[68] DSG Section 21.

Please note: The DSB has—based on the DSG[69] issued white lists and black lists for DPIAs.[70]

The DSB shall approve "Codes of Conduct" in terms of GDPR Art. 40.[71]

The DSB must make public the criteria to be accredited pursuant to GDPR Art. 57(1)(p) (accreditation in the context of GDPR Arts. 41, 43) by way of an ordinance.

The DSB shall also act as the only national accreditation body pursuant to GDPR Art. 43(1)(a).

Investigative Powers of Supervisory Authorities

GDPR Provisions

Article 58(1) of the GDPR defines the investigative powers of supervisory authorities. The following powers are particularly relevant to controllers and processors:

- To order the controller and data processor to provide any information the supervisory authority requires for the performance of its tasks;
- To carry out investigations in the form of data protection audits;
- To review certifications issued by certifying bodies;
- To notify controllers and processors of alleged infringement of GDPR;
- To obtain from the controller and processor access to all personal data and to all information necessary for the performance of its tasks; and
- Obtain access to any premises, including data processing equipment and means, in conformity with EU law or Member State procedural law.

Austria-Specific Additional Provisions

When investigating a processing activity, the DSB may order the controller and the processor of the reviewed data processing to provide all necessary information and access to data processing and relevant documents.[72] The controller or the processor must provide the necessary support. The supervisory activity must be carried out with the greatest possible protection of the rights of the controller or the processor and third parties.

For the purposes of access, after notification of the proprietor of premises and the controller or the processor, the DSB is authorized to:

- Enter premises in which data processing is being carried out;
- Out data processing into operation;

[69]DSG Section 21(3): "*The Data Protection Authority shall make public, by way of a regulation, the criteria to be specified pursuant to Article 57 para. 1 (p) of the General Data Protection Regulation.*"

[70] https://www.dsb.gv.at/verordnungen-in-osterreich.

[71] https://www.dsb.gv.at/genehmigung-von-verhaltensregeln.

[72]DSG Section 22(1) to (3).

- Carry out the processing to be reviewed, and
- Produce copies of data storage media to the extent absolutely necessary for the exercise of the supervisory powers.

Information that the DSB or persons authorized by it receive during their supervisory function may be used only for the supervision within the framework of the execution of data protection provisions. Moreover, the obligation of confidentiality (generally) also exists *vis-à-vis* the courts and administrative authorities, including the tax authorities.

Corrective Powers of Supervisory Authorities

GDPR Provisions

In addition to investigative powers, supervisory authorities have corrective powers listed in GDPR Art. 58(2). Among those corrective powers, the following are noteworthy:

- To issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR;
- To issue reprimands to a controller or processor where processing operations have infringed provisions of GDPR;
- To order the controller or processor to comply with data subjects' requests to exercise their rights pursuant to GDPR;
- To order a controller or processor to bring processing operations into compliance with GDPR, where appropriate, in a specified manner and within a specified period;
- To order a controller to communicate a personal data breach to the data subject;
- To impose a temporary or definitive limitation, including a ban on processing;
- To order the rectification or erasure of data or restriction of processing, and the notification of such actions to recipients to whom the data have been disclosed;
- Withdraw a certification issued by a certification body, or to order the certification body to withdraw it, or to order a certification body not to issue the certification;
- To impose an administrative fine; and
- To order the suspension of data flows to a recipient in a third country or to an international organization.

Austria-Specific Additional Provisions

In Austria, additional requirements are introduced in the DSB.[73] If there is a significant direct risk to the secrecy or confidentiality interests of a data subject meriting protection (imminent danger in the delay) due to a data processing operation, the DSB may forbid the continuation of the data processing per decision.[74] If it is technically possible, reasonable with regard to the purpose of the data processing, and sufficient in order to remove the imminent

[73]DSG Section 22(4).

[74]General Administrative Law Act 1991—AVG Section 57(1).

danger, the continuation may be only partially forbidden.

The DSB may also, upon request of a data subject, order a limitation on the processing (GDPR Art. 18) per decision if the Controller does not fulfil this obligation on time.

If a prohibition is not immediately complied with, the DSB must proceed pursuant to GDPR Art. 83(5).

Pursuant to the DSG,[75] the DSB must apply the catalogue of GDPR Art. 83(2) to (6) in such a way that proportionality is maintained. In particular in the event of first-time violations, the DSB shall exercise its remedial powers, in particular by warning, in accordance with GDPR Art. 58.

Authorization and Advisory Powers of Supervisory Authorities

GDPR Provisions

Under GDPR Art. 58(3), each supervisory authority is granted authorization and advisory powers, in particular, the power to approve BCR and advise controllers in accordance with the prior consultation procedure. They also have an important role in issuing opinions and approving draft codes or conduct and accreditation of certification bodies.

GDPR Art. 58(5) also requires each Member State to provide by law that its supervisory authority has the power to bring infringements of GDPR to the attention of the judicial authorities and, when appropriate, to commence or engage in legal proceedings to enforce the GDPR.

Austria-Specific Additional Provisions

Pursuant to the DSG,[76] the DSB must apply the catalogue of provisions in GDPR Art. 83(2) to (6) in such a way that proportionality is maintained. In particular in the event of first-time violations, the DSB will exercise its remedial powers, in particular by warning, in accordance with GDPR Art. 58.

However, the DSB has the authority to impose monetary fines *vis-à-vis* natural and legal persons within the scope of its competence.[77] Decisions of the DSB that are of general importance to the general public must be published by the DSB in an appropriate manner taking into consideration the requirements of official secrecy.[78]

Mutual Assistance, Cooperation with Other Supervisory Authorities

GDPR Art. 61 requires that the supervisory authorities provide each other with relevant information and mutual assistance to implement and apply the GDPR in a consistent manner

[75]DSG Section 11.

[76]DSG Section 11.

[77]DSG Section 22(5).

[78]DSG Section 23(2).

and that they put in place measures for effective cooperation with one another. This mutual assistance covers, in particular, responding to information requests and implementing supervisory measures, such as requests to carry out prior authorizations and consultations, inspections, and investigations.

Lead Supervisory Authority

Under GDPR Art. 56(1), when a controller or processor operates in several Member States, the supervisory authority of the main establishment of the controller or processor is competent to act as "lead supervisory authority" for the crossborder processing carried out by that controller or processor to handle disputes that involve establishments in several Member States. However, if the subject matter of a dispute relates only to an establishment in its Member State or substantially affects data subjects only in one Member State, the supervisory authority of that member state is competent to handle that complaint. GDPR Art. 56(2).

Austria Political Advisory Council

In Austria, in addition to providing for a Data Supervisory Authority, the Austrian DSG provides for a "political advisor board," so called Data Protection Council:[79]

The Data Protection Council is empowered to comment on questions of fundamental importance for data protection, promote the uniform further development of data protection, and advise the Federal Government on legal policy in the case of projects relevant to data protection.

To fulfil its duties the Data Protection Council:

- Can make recommendations relating to data protection to the Federal Government and the federal ministers;
- Can prepare opinions or commission such opinions;
- Is given the opportunity to comment on draft bills of federal ministries, insofar as these are significant for data protection law, and on regulations to be implemented by the Federal Government concerning essential issues of data protection;
- Has the right to request information and reports from Public-Sector Controllers insofar as this is necessary to evaluate, from the viewpoint of data protection law, projects of significant impact on data protection in Austria; and
- Will publish its observations, concerns and suggestions and submit them to the Public-Sector Controllers.

Complaints, Disputes

Data subjects have extensive rights under the GDPR in connection with complaints and disputes.

[79]DSG Sections 14 to 17.

Right to Lodge a Complaint with a Supervisory Authority

GDPR Provisions

GDPR Art. 77 grants data subjects the right to lodge a complaint with a supervisory authority. If the data subject believes that the processing of his or her personal data infringes the GDPR, he or she may lodge a complaint in the EU Member State where he or she resides, where his or her place of work is, or where the alleged infringement took place. This right is in addition to any other administrative or judicial remedy that an individual might seek.

The supervisory authority with which the complaint has been lodged must inform the complainant on the progress and the outcome of the complaint, including the possibility of a judicial remedy.

Austria-Specific Additional Provisions

In addition to the above, in Austria, every data subject has the right to lodge a complaint with the DSB if the data subject considers that the processing of personal data relating to the data subject infringes the GDPR or the DSG.[80] The complaint must include:

- The name of the right believed to have been infringed;
- To the extent reasonable, the name of the legal body or organ to whom the claimed infringement can be attributed (respondent);
- The facts from which the infringement is derived;
- The facts on which the claim of infringement is based;
- A request to recognize the claimed infringement; and
- The information necessary to assess whether the complaint was lodged in a timely manner.

The right to have a complaint examined expires if the complaint is not lodged within a year after the data subject having gained knowledge of the incident that gave rise to the complaint, but no later than within three years after the incident allegedly occurred. Late complaints will be rejected by the DSB.

A complaint must include the application on which it is based and a response by the respondent (if available). The DSB may provide further support in case of a complaint at the request of the data subject.

The DSB must inform the complainant on the progress and the outcome of the complaint, including the possibility of a judicial remedy.

If the complaint is proven justified, it will be granted. If an infringement is attributed to a Controller from the private sector, the Controller will be ordered to grant the request of the complainant for access, rectification, erasure, restriction, or data portability to the extent necessary to remedy the determined infringement. If the complaint is proven to be unjustified, it will be denied.

A respondent may subsequently remedy the claimed infringement until the end of the proceedings before the DSB by granting the complainant's requests. If the DSB believes that

[80]DSG Sections 24 and 25.

the claim is invalid, the complainant will be heard in this regard. Concurrently, the complainant will be made aware of the fact that the proceedings will be informally terminated if the complainant cannot substantiate within a reasonable period why the complainant believes that the claimed infringement is still not remedied (at least in part). If such a statement of the complainant changes the matter fundamentally, the original complaint will be withdrawn and simultaneously a new complaint will be filed. In this case as well, the old complaints procedure will be informally terminated, and the complainant will be notified thereof. Late statements will not be taken into account.

To the extent required, the DSB can engage official experts to assist in the proceedings.

If, in the context of a complaint, the complainant satisfactorily demonstrates a serious infringement of his or her interests in confidentiality that deserve protection due to the processing of the complainant's personal data, the DSB may prohibit the continuation of the data processing operation by an administrative decision.

If the correctness of personal data is disputed in proceedings, the respondent to the complaint must submit, by the end of the proceedings, a note stating that the correctness is disputed. If required, the DSB will order, by an administrative decision, such note to be submitted at the request of the complainant.

If a Controller invokes a restriction (GDPR Art. 23) in relation to the DSB, the DSB will examine the lawfulness of the application of the restrictions. If the DSB comes to the conclusion that it was not justified in keeping the processed personal data secret from the data subject, the disclosure of the data will be ordered by an administrative decision. If the administrative decision by the DSB is not complied with within eight weeks, the DSB will disclose the personal data to the data subject and will communicate to the data subject the desired information or inform the data subject of the personal data that have already been rectified or erased.

The complainant will be informed by the DSB within three months from filing the complaint about the progress and outcome of the investigation.

Each data subject may submit a matter to the Federal Administrative Court if the DSB does not address the complaint or the data subject has not been informed of the progress or outcome of the complaint within three months.

Right to Effective Judicial Remedy Against Supervisory Authority

GDPR Provisions

GDPR Art. 78 grants data subjects the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. This right is in addition to any other administrative or nonjudicial remedy that an individual might seek.

Data subjects also have the right to an effective judicial remedy when the competent supervisory authority does not handle a complaint or does not inform the data subject on the progress or outcome of the complaint within three months. In these cases, the proceedings against a supervisory authority must be brought before the courts of the Member State where the supervisory authority is established.

Austria-Specific Additional Provisions

The Federal Administrative Court decides through a panel of judges on complaints against administrative decisions on the ground of a breach of the duty to provide information and the duty to reach a decision of the DSB.[81]

In the case of a dispute between an employer and an employee, the panel of judges consists of a chair and one expert lay judge each from among employers and from among employees. The expert lay judges is appointed on the basis of a proposal by the Austrian Federal Economic Chamber and the Federal Chamber of Labor. Appropriate arrangements will be made so that a sufficient number of expert lay judges is available in due time. The expert lay judges must have at least five years of relevant professional experience and special knowledge of data protection law. The chair of the panel must provide all documents relevant to the decision to the expert lay judges without delay, or, if this is impractical or strictly necessary to safeguard the confidentiality of the documents, make them available in some other way.

Where proceedings are brought against an administrative decision of the DSB that was preceded by an opinion or a decision of the European Data Protection Board under the consistency mechanism, the DSB will forward that opinion or decision to the Federal Administrative Court.

Right to an Effective Judicial Remedy Against Controller or Processor

GDPR Provisions

Under GDPR Art. 79, data subjects have the right to an effective judicial remedy against a controller or processor if they consider that their personal data has been processed in non-compliance with GDPR. This right is in addition to their right to exercise any available administrative or nonjudicial remedy, including the right to lodge a complaint with a supervisory authority.

The proceedings against a data controller or a data processor may be brought before the courts of the EU Member State where the data controller or data processor has an establishment or where the data subject has his or her habitual residence.

Austria-Specific Additional Provisions

In Austria, the Regional Court entrusted with exercising jurisdiction in civil matters in whose judicial district the plaintiff (applicant) has his usual place of residence or registered office has first-instance jurisdiction over actions for compensation.[82] Actions (requests) may, however, also be brought before the Regional Court in whose judicial district the defendant has his usual place of residence or registered office or a branch office.

[81]DSG Section 27.

[82]DSG Section 29(2).

Right to Mandate Not-for-Profit Organizations to Lodge a Complaint

GDPR Provisions

GDPR Art. 80 grants each data subject the right to mandate certain not-for-profit entities, organizations, or associations to do the following on the data subject's behalf:

- To lodge a complaint;
- To exercise the right:
  - To lodge a complaint with a supervisory authority (under GDPR Art. 77);
  - To have an effective judicial remedy against a supervisory authority that did not handle the data subject's complaint or failed to inform the data subjects on the progress or outcome of the complaint (under GDPR Art. 78); and
  - To have an effective judicial remedy against a data controller or data processor; where the data subject considers that his rights have been infringed as a result of the processing of his data (under GDPR Art. 79); and
- To exercise the right to receive compensation from the processor or controller for the damage suffered (under GDPR Art. 82).

To qualify to perform these activities, the not-for-profit entity must have statutory objectives in the public interest and be active in the protection of rights and freedoms with regard to personal data.

Member States may also provide that any not-for-profit entity (within the limits set forth above) may, without having received a mandate from a data subject, lodge in that Member State a complaint with the competent supervisory authority and to exercise the right to an effective judicial remedy against a data controller, data processor, or supervisory authority if that not-for-profit entity considers that the rights of a data subject under the GDPR have been infringed as a result of the processing his or her data.

Austria-Specific Additional Provisions

In Austria,[83] the data subject also has the right to mandate a not-for-profit body, organization, or association[84] that has been properly constituted, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights on his or her behalf, however not to exercise the right to receive compensation.

The Austrian Supreme Court9 ruled that § 28 DSG (representation of data subjects by a data protection association) exclusively stipulates the representation of a data subjects in proceedings in front of the DSB – Austrian Data Protection Authority. Under Art 80(2) GDPR,

[83]DSG Section 28.

[84]DSG Section 28.

[9] OGH 26.11.2019, 4Ob84/19k.

Member States can provide that certain institutions enforce the rights even without the data subject's instructions. This shows that unauthorized prosecution of data protection violations by third parties (associations) is only permitted if the national legislator expressly provides for such a possibility. This means that the respective member state must explicitly regulate a collective action for data protection claims. Austria has not made use of this “opening clause”. Thus, no class action lawsuit is envisaged to enforce claims under the GDPR in Austria.

[5] Right to Compensation; Liability

GDPR Provisions

GDPR Art. 82 grants any person who has suffered damage as a result of an infringement of the GDPR the right to receive compensation from the data controller or data processor for the damage suffered. The rules of allocation of liability, set forth in GDPR Art. 82, include:

- Any controller involved in processing is liable for the damage caused by processing that infringes GDPR;
- Any processor is liable for the damage caused by the processing only if it did not comply with its obligations under GDPR or if it has acted outside, or contrary to, lawful instructions of the data controller;
- A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the damage;
- If more than one controller or processor, or both a controller and a processor, are involved in the same processing and if they are responsible for any damage caused by the processing, they are jointly and severally held liable for the entire damage;
- If a controller or processor has paid full compensation for the damage suffered, it is entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage;
- Proceedings for exercising the right to receive compensation must be brought in the courts of the EU Member State where the case is brought.

Austria-Specific Additional Provisions

Under Austrian law,[85] any person who has suffered material or non-material damage as a result of an infringement of the GDPR or against the DSG has the right to receive compensation from the Controller or the Processor for the damage suffered pursuant to GDPR Art. 82. For these liability claims, the general provisions of civil law apply in each individual case.

The Regional Court for Civil Law, in which the plaintiff (applicant) has his place of residence or seat, is the competent court in the first instance for liability claims. Claims (applications) may, however, also be brought before the Regional Court in whose jurisdiction the defendant has his place of residence or seat or branch.

See [P][14] for Austrian case law on (immaterial) damages and burden of proof.

[85] DSG Section 29.

Administrative Fines

General Conditions for Imposing Administrative Fines

GDPR Provisions

GDPR Art. 83 grants the supervisory authority the responsibility to ensure that administrative fine for infringements of the GDPR are effective, proportionate, and dissuasive.

Depending on the circumstances, administrative fines are imposed in addition to, or instead of, measures that the supervisory authority may have taken directly, such as ordering an entity to bring processing into compliance or to communicate a breach of security to the data subject.

When deciding whether to impose an administrative fine and its amount, the supervisory authority must take into account the surrounding circumstances, such as:

- The nature, gravity, and duration of the infringement taking into account the nature, scope, or purpose of the processing, the number of data subjects affected, and the level of damage suffered by them;
- Whether the infringement was intentional or negligent;
- Any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- The degree of responsibility of the controller or processor, taking into account technical and organizational measures implemented by them;
- Any relevant previous infringements by the same entity;
- The degree of cooperation with the supervisory authority to remedy the infringement and mitigate the possible adverse effects of the infringement;
- The categories of personal data affected;
- The manner in which the infringement became known to the supervisory authority, in particular whether, and to what extent, the controller or processor gave notice of the infringement;
- If the controller or processor has received prior warning or recommendation from the supervisory authority with respect to the same subject matter, the degree of compliance with those pre-exiting requirements;
- Adherence to approved codes of conduct or certification mechanisms; and
- Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

If an entity intentionally or negligently, for the same or linked processing operations, infringes several provisions of GDPR, the total amount of the administrative fine may not exceed the amount specified for the gravest infringement.

Austria-Specific Additional Provisions

In Austria, the DSB[86] can impose administrative fines on a legal person if infringements of provisions of the GDPR/DSG were committed by persons who acted either individually or as part of an executive body of the legal person and have a leading position within the legal person on the basis of:

- A power of representation of the legal person;
- The authority to take decisions on behalf of the legal person; or
- The authority to exercise control within the legal person.

Legal persons may also be held responsible for infringements if such infringements by a person acting for the legal person were made possible by a lack of supervision or unless the act constitutes a criminal offence within the jurisdiction of the courts.

The VwGH ruled[10] that the Administrative Penal Code (Verwaltungsstrafgesetz (VStG)) applies to official procedures of the Data Protection Authority (DPA) for the imposition of monetary fines pursuant to Art 83 GDPR. The provisions of § 30 (1) to 3 Data Protection Act are necessary in order to ensure the full enforcement of Art 83 GDPR in national law because the VstG only provides for proceedings for the criminal liability of natural persons; Art 83 GDPR, in contrast, does not distinguish between infringements by legal and natural persons. However, in the judgement, for the criminal liability of legal persons for conduct by natural persons imputable to them for the determination of an act of persecution within the meaning of §§ 31 and 32 VStG respectively punishment within the meaning of § 44a VStG by the Data Protection Authority, a criminal, unlawful and culpable conduct by a natural person mentioned by name, must have been recorded.

The DSB will refrain from imposing a fine on a "responsible party,"[87] if an administrative penalty has already been imposed on the legal person for the same infringement and there are no particular circumstances opposing the refraining from imposing a fine.

Administrative fines imposed will be received by the Federal Government and will be collected pursuant to the provisions on the collection of judicial fines. Final administrative decisions by the DSB are writs of enforcement. Approval and implementation of enforcement must be requested on the basis of the writ of enforcement by the DSB from the district court in whose judicial district the obligated party has his or her general place of jurisdiction or from the enforcing court.

Administrative fines cannot be imposed on authorities and public entities.

Amount of Administrative Fines

GDPR Provisions

The GDPR defines two levels of fines, which apply to two categories of offenses.

10 Million Euros or 2 Percent Annual Turnover Fines.

Infringement of the following provisions are subject to administrative fines of up to 10 million

[86]DSG Sections 30 and 62.

[10] VwGH 12.05.2020, Ro 2019/04/0229.

[87]Administrative Penal Act 1991 Section 9.

euros or up to 2 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- Violation of GDPR Art. 8 regarding the collection of children's personal data;
- Failure to use data processing by design and by default as forth in GDPR Art. 25;
- Failure to designate a data protection officer, if required (GDPR Art. 35); and
- Failure to meet the requirements of a certification body (GDPR Arts. 42, 43).

20 Million Euros or 4 Percent Annual Turnover Fines.

Infringements of other provisions are subject to administrative fines of up to 20 million euros or up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

These include, for example,

- Failure to meet the basic principles for processing, including the conditions for consent (GDPR Arts. 5, 6, 7, and 9);
- Infringement of data subjects' rights of information, access to their data, right of rectification, right of erasure, right to restrict the processing of their data, right to data portability, right to object to the processing of their data; right not to be subject to a decision based solely on automated processing, including profiling (GDPR Arts. 12 to 22);
- Failure to comply with the rules pertaining to the transfer of personal data to a third country (GDPR Arts. 44 to 49); and
- Noncompliance with an order or a limitation on processing or the suspension of data flows by the supervisory authority (GDPR Art. 58).

Austria-Specific Additional Provisions

Criminal Penalties.

Anyone who, with the intention to unlawfully profit or to damage someone's right pursuant to the DSG unlawfully uses personal data that has solely been entrusted to him or made available to him on the basis of his professional occupation, although the data subject has a protected interest in the confidentiality of this data, will be, if the act is not punishable by a more severe penalty according to another provision, punished by the Penal Court with a prison sentence of up to one year or a monetary penalty of up to 720 average daily penalty units.[88]

Administrative Penalties.

If the act is not an offense pursuant to GDPR Art. 83 or does not carry the threat of a more severe penalty according to other administrative criminal provisions, an administrative offense is punishable by a monetary penalty in the amount of up to EUR 50,000, if committed by someone who (i) intentionally gains illegal access to data or intentionally maintains noticeably illegal access, (ii) intentionally transfers data in breach of Data Secrecy, (iii) gains access to personal data under false pretenses, (iv) carries out image processing contrary to the

[88]DSG Section 63.

provisions, or (v) denies access.[89]

An attempt is punishable by law.

Notable Cases and Enforcement Actions in Austria

The Austrian Data Protection Authority and Courts has been assuming the immediate applicability of the GDPR (also to past events and pending proceedings) since May 25, 2018, as Section 69 DSG does not provide a transitional period. Therefore, Austrian case law provides (most probably) the first decisions of higher instances—and even of the Austrian Highest Courts—on the rules and regulations of the GDPR.

Customer Request to Obtain a Historical Bank Statement

The Austrian Data Protection Authority (DSB) issued a decision applying the GDPR on June 26, 2018. According to the DSB, Art. 15 GDPR covers the customer's request to obtain the customer's historical bank account statements free of charge**,** as no third-party rights are endangered.[90]

Validity of Consent

According to the Austrian Supreme Court (OGH), the GDPR does not stipulate an absolute prohibition of coupling. However, it must generally be assumed that the granting of consent is not voluntary if there are no special circumstances in the individual case that indicate voluntariness of the consent.[91] However, the DSB ruled that it must be clear that the consent is given freely; therefore, forms must not give the impression that the consent is required by the contract, for example, for becoming a member of an automotive touring club.[92]

Use of Dashboard Camera

The DSB ruled (as in several decisions before) that the use of dash-cams is generally not in line with the legal data protection framework.[93]

Right to Non-Disclosure of Personal Data; Anonymization v. Deletion, Pseudonymization

According to the Supreme Administrative Court (VwGH), the DSG provides a comprehensive right to non-disclosure of personal data independent of the technical organizational conditions of their processing, thus also in the case of non-automated processed data.[94]

However, the DSB ruled that, instead of deletion of the entire data, an anonymization of

[89]DSG Section 30, 62.

[90]DSB-D122.844/0006-DSB/2018, dated 21/06/2018.

[91]OGH 31/08/2018, 6 Ob 140/18h.

[92]VwGH 28/02/2018, Ra 2015/04/0087; compare in this regard ECJ 10/07/2018, C-25/17—Jehova.

[93]DSB-D485.000/0001-DSB/2018-II, dated 09/07/2018.

[94]DSB-D213.642/0002-DSB/2018, dated 31/07/2018.

the personal data leads to the consequence that the data protection regulation do not apply (anymore).[95] Furthermore, the DSB can only make an ex-post determination of a breach of the fundamental right to non-disclosure. With regard to a breach of the fundamental right to non-disclosure through a "neglected pseudonymization," it must be noted that no right can be inferred from the GDPR according to which a concerned person can demand specific data security measures within the meaning of the GDPR from a controller. Similarly, a concerned person cannot demand specific measures for data minimization.[96]

Unlawfulness of Data Processing by Breach of "Non-Data Protection" Provisions

According to the VwGH, for the assessment of the unlawfulness of data processing (according to the legislation before the GDPR), provisions outside of data protection law are also to be taken into consideration insofar as they deal with the prohibition of (a certain type) data use.[97]

Commercial Messages (TKG vs Data Protection Law)

According to the Data Protection Authority, the ePrivacy Directive, namely its implementation in the Austrian Telecommunications Act 2003, takes precedence over the DSG, namely the GDPR as a *lex specialis*.[98] Nevertheless, the infringement of the spamming-prohibition laid down in the Austrian Telecommunication Act may (also) be an infringement of the data protection law framework.[99]

DSB: Choice of Punishment, but Formal Requirements

According to the VwGH, the DSB has broad discretion with regard to the choice of punishment, but it requires transparent explanations that enable the VwGH an (if only restrictive) assessment of whether the discretion was exercised within the meaning of the law.[100]

However, the VwGH ruled[11] that the Administrative Penal Code (Verwaltungsstrafgesetz (VStG)) applies to official procedures of the Data Protection Authority (DPA) for the imposition of monetary fines pursuant to Art 83 GDPR. The provisions of § 30 (1) to 3 Data Protection Act are necessary in order to ensure the full enforcement of Art 83 GDPR in national law because the VstG only provides for proceedings for the criminal liability of natural persons; Art 83 GDPR, in contrast, does not distinguish between infringements by legal and natural persons. However, in the judgement, for the criminal liability of legal persons for conduct by natural persons imputable to them for the determination of an act of persecution within the meaning of §§ 31 and 32 VStG respectively punishment within the meaning of § 44a VStG by the Data

[95]DSB-D123.270/0009-DSB/2018, dated 05/12/2018.

[96]DSB-D123.070/0005-DSB/2018, dated 13/9/2018.

[97]VwGH 26/06/2018, Ra 2017/04/0032.

[98]DSB-D122.931/0003-DSB/2018, dated 30/11/2018.

[99]DSB-D130.033/0003-DSB/2019, dated 07/03/2019.

[100]VwGH 16/05/2018, Ra 2017/04/0080.

[11] VwGH 12.05.2020, Ro 2019/04/0229.

Protection Authority, a criminal, unlawful and culpable conduct by a natural person mentioned by name, must have been recorded.

Identification of the Data Subject and Right to (Trade) Secrets when denying the Data Subject's Rights

According the VwGH, the new legislation does not provide for stricter provisions with regard to identification of the data subject when requesting her or his rights: pursuant to the GDPR, the Controller may, if it has justified doubts regarding the identity of a natural person who has filed a request, ask for additional information that may be necessary to confirm the identity of the concerned person. A content-related refusal to provide information cannot be justified with this subsequently.[101] Therefore, the controller has to check and has to give reasoning on a case-by-case basis when referring to the obligation and/or right to (trade) secrets when denying the data subject's rights provided by the GDPR.

Court-Certified Experts as Controllers

The Federal Administrative Court is of the legal view—contrary to the explanatory notes to the law—that court-certified experts are at a minimum to be viewed as data protection controllers together with the court that appointed them to prepare an expert opinion, as they decide on the methods independently and assuming responsibility for what they do.[102]

Legal Persons are subject to Austrian Data Protection Law

The Regional Administrative Court Tyrol (T-LVwG) issued a decision that the DSG still protects legal persons after the GDPR amendment: "*In this respect, there is also within the meaning of DSG Section 1—which is still applicable to legal persons—a corresponding legitimate interest in privacy* […]."[103]

Retention Period based on Specific Legal Provisions

The DSB had the opportunity to rule on retention periods several times:

- According to the DSB, the right to deletion pursuant to the GDPR is not an option if processing is required in one of the cases in the exhaustive list of GDPR Art. 17(3)(a) to (e). The case "defence of legal claims" is in any case temporally relevant if the assertion, exercise, or defence of (respectively against) legal claims is already taking place or certainly will take place; the mere abstract possibility of legal disputes is, however, not sufficient. However, a retention period of seven months for job application data is legitimate, as the anti-discrimination laws provide a statute of limitations of six months.[104]
- Whenever laws provide specific retention periods**,** they must be strictly applied; for

[101]BVwG 27/09/2018, W214 2127449-1.

[102]BVwG 27/09/2018, W214 2196366-2; compare in this regard: ECJ 05/07/2018, C-210/16—Facebook Insights.

[103]LVwG-2018/29/0312-5, dated 02/11/2018.

[104]DSB-D123.085/0003-DSB/2018, dated 27/8/2018.

example, in the telecommunications sector.[105]

- The mere abstract possible need in the future to contact a customer does not justify a retention of the contact data.[106]

Formalities of Data Subject Requests

Finally, the DSB issued several decisions on the formalities of a data subject's request.[107]

Deletion of Criminal Proceedings and Anonymization of Published Disciplinary Findings

The OGH ruled on the questions of when and under what conditions the personal data of criminal proceeding have to be deleted.[108]

The Austrian Supreme Court ruled[12] as follows with regard to anonymization of published disciplinary findings: By a disciplinary decision of the Supreme Court of 4 July 2019, the complainant - a judge - was found guilty of violating the judicial disciplinary obligation to behave out of office in such a way that the trust in the administration of justice and the reputation of the profession is not jeopardized by various tweets, as detailed below, and thereby committed a breach of duty, for which he was ordered to pay a fine of one month's salary and to reimburse costs. The disciplinary decision was published on 5 September 2019 in the Federal Legal Information System (RIS) in anonymized form. The complainant's complaint is directed against this publication. In his appeal, he essentially argues that in the published findings, his first name is written out in full and only his surname is abbreviated with an "H. To this end, the Supreme Court has considered: The complaint is not justified - on the following grounds: Pursuant to § 85 (1) GOG, anyone who has been violated in the fundamental right to data protection by an organ acting in the exercise of its judicial activity in matters of jurisdiction in civil cases and in the administration of justice to be dealt with in senates may request the Federal Government to establish this violation. The higher court of first instance shall have jurisdiction to rule on this appeal (§ 85 (2) sentence 1 GOG). Pursuant to § 133a RStDG, final decisions of the disciplinary courts that terminate the proceedings are to be published immediately in the RIS in anonymized form by the respective chairman. In the present case, the disciplinary hearing before the Supreme Court was public; for this reason alone, publication of the disciplinary findings was mandatory under § 15(1) OGHG. As the Supreme Court has stated in connection with provisional proceedings, in both non-contentious and contentious proceedings, the parties must accept identifying publication if there were no legally recognized confidentiality interests and the hearing was thus public anyway. In this (standard) case, the public's interest in information weighs more heavily than the anonymity interest of the participants according to the evaluation of the law.

[105]DSB-D216.471/0001-DSB/2018, dated 28/05/2018.

[106]DSB-D216.580/0002- DSB/2018, dated 28/05/2018.

[107]DSB-D123.627/0003-DSB/2018, dated 02/01/2019; DSB-D123.512/0004-DSB/2018, dated 11/01/2019.

[108]OGH 02.04.2019, 11Os69/18h.

[12] OGH 27.11.2019, 6Nc30/19t.

Requirements for Claims for (Immaterial) Damages and Burden of Proof

The Higher Regional Court of Innsbruck[13] ruled with regard to immaterial damages for breaches of data protection: The plaintiff requested EUR 2,500 in the claim first filed with the preliminary court on the 29.3.2019 from the title of immaterial damages and based this on the following, in his view unlawful conduct of the defendant: The defendant processed information regarding alleged party political preferences of the plaintiff, i.e. specific categories of data: the court ruled in this regard: In order to ensure full protection of the persons concerned, Art 82 GDPR provides for an independent liability provision for the violation of the protection of personal data, which gives rise to a direct tortious claim for damages. Art 82 GDPR (in conjunction with § 29 (1) Data Protection Act) thus constitutes a tort liability rule in its own right which enables the persons concerned, who do not have a direct legal relationship with the injuring party, to obtain full and effective compensation from the latter for the damage suffered. National tort law therefore supplements the liability for damages under the GDPR (§ 29 (1) 2nd sentence Data Protection Act), so that these are decisive for the general requirements for a claim, unless the GDPR contains special provisions. In the case of a tortious claim for damages, the plaintiff must assert and prove the conditions on which liability is based. These include the occurrence of a (material or immaterial) damage, the violation of a norm, i.e. the (objective) unlawfulness by the injuring party as well as the (co-)causation of the injuring party's conduct in the damage that occurred in the sense of an adequate causality. The requirement of actual damage also precludes the award of symbolic damages. For this reason, a claim for immaterial damages must be based on the fact that there has been an actual impact to the emotional world of the injured party. Immaterial damage is therefore damage that cannot be measured in money terms and which is caused by personal impairments. In Recital 75 of the GDPR, several circumstances are mentioned which could constitute damages for the persons concerned, such as discrimination, identity theft, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, any other significant economic or social disadvantage. Although, according to the unambiguous wording of Art 82 GDPR, no serious violation of the right of personality is required in order to claim non-material damage, the assumption that any violation of the GDPR leads to an obligation to compensate solely for general preventive reasons is incorrect. A breach of data protection must in any event affect the emotional sphere of the injured party in order to be able to speak of non-material damage (Art 82 (1) GDPR) caused by a breach of the GDPR. The Higher Regional Court of Innsbruck ultimately concludes that the plaintiff failed, in the first instance, to sufficiently claim and prove non-material damage suffered by him as a result of the defendant's alleged infringements. In the opinion of the court, this means that although insignificant impairments do not remain without sanction - then there is also a legally enforceable right to injunctive relief and removal with regard to the infringements of his rights under the GDPR alleged by the plaintiff - these infringements do not per se already lead to an obligation to compensate for the immaterial damage.

The Austrian Supreme Court[14] ruled on the burden of proof for claims for damages under data protection law: Art 82 (3) GDPR provides for a reversal of the burden of proof, according to which no liability exists if the person responsible or processor proves that he is in no way responsible for the event giving rise to the damage. Art 82 GDPR is to be seen as a complement to national tort law and as a kind of lex specialis of a data protection tort law. The

[13] OLG Innsbruck 13.02.2020, 1R182/19b.

[14] OGH 27.11.2019, 6Ob217/19h.

applicant did not even succeed in proving the damage, nor, moreover, in proving causality. The use of prima facie evidence is also out of the question: prima facie evidence is considered appropriate in cases in which the party required to provide evidence cannot reasonably be expected to provide comprehensive and concrete evidence because the circumstances in need of proof lie solely in the sphere of the other party, can only be known to the latter and can therefore only be proven by him.

Digital Peephole without Recording Function

The Federal Administrative Court[15] ruled as follows on the question of the admissibility of a "digital peephole without recording function" regarding the Austrian special provisions on image processing: The recognizing senate precedes its assumption that there is no room for the application of §§ 12 and 13 Data Protection Act due to the lack of a corresponding opening clause in the GDPR and that they must therefore not be applied. The complaint in question must therefore be examined solely on the basis of the GDPR: In the appellant's front door, instead of a regular peephole, there is a digital peephole with a monitor without a recording function from the brand 'Yale', which transmits a 10-second recording in real time at the touch of a button. The digital peephole does not save/record the transmitted images and as such cannot be distinguished from a regular peephole from the outside. According to the legal definition of Art 4 (2) GDPR, the term "processing" consists of a general definition and a demonstrative list of different types of processing. In the present case, there is real-time image transmission (real-time monitoring), which is characterized by the fact that images are transmitted from one location to another without being stored. Since this type of image transmission represents a process carried out with an automated procedure in connection with personal data and thus falls within the general definition of processing under Art. 4 No. 2 GDPR, it is in any case covered by the meaning of this term. According to Art. 6 (1) lit. f GDPR, such processing may be lawful if it is necessary to safeguard the legitimate interests of the controller or of a third party, provided that the interests or fundamental rights and freedoms of the data subjects do not prevail. In the present case, it should be pointed out that the installation of a (regular or digital) peephole is basically a suitable means of detecting potential dangers before the door is opened, although there is no more moderate means available for this purpose. As explained above, although the use of a digital peephole involves real-time monitoring, such systems - without the storage and recording of image files - significantly reduce the risk to confidentiality interests worthy of protection. A constant pressure to monitor cannot be generated by this, nor by a regular peephole whose intensity of intervention it does not exceed. The present data processing is therefore justified in the light of the GDPR, since according to its Art. 6 (1) lit. f GDPR the processing is necessary to safeguard the legitimate interests (namely the protection purpose) of the controller and these outweigh the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.

Excessive Provision of Information by the Public Prosecutor's Office and on the Question of the Possible Limits of Competence of the DSB regarding Courts

The Federal Administrative Court[16] ruled as follows on an excessive provision of information by the public prosecutor's office and on the question of the possible limits of

[15] BVwG 18.12.2019, W211 2209492-1.

[16] BVwG 18.12.2019, W211 2213604-1/3E.

competence of the data protection authority as follows: Not only the contents of the file requested by a lawyer were transmitted, but also completely different investigatory content (with health records). Following the lawyer's submission, the Data Protection Authority initiated an official investigation pursuant to § 32 (1) 3 and § 34 (5) of the Data Protection Act. The Federal Administrative Court ruled that the processing of personal data for the purposes of investigating and prosecuting criminal offences is regulated in the 3rd main section of the Data Protection Act in §§ 36 ff Data Protection Act. This implemented into national law the GDPR adopted on 25 May 2018 together with the GDPR specifically for the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the enforcement of sentences. Pursuant to § 31 (1) 1st sentence Data Protection Act, the Data Protection Authority is established as the national supervisory authority for the area of application specified in § 36 (1) Data Protection Act. This complies with the requirement in Article 41(1) of the Directive that the supervisory authority (Data Protection Authority) should be responsible for both the scope of the GDPR and the Directive. According to § 31 (1) 2nd sentence Data Protection Act, the Data Protection Authority is (however) not competent to supervise processing operations carried out by courts in the course of their judicial activities. In the present case, the appellant takes the view that, as a public prosecutor's office, she is covered by this exception to the competence of the Data Protection Authority. The Federal Administrative Court, however, decided that the Austrian legislator, in conformity with the implementation of the Directive, did not legally exempt from the competence of the Data Protection Authority (in § 31(1) of the Data Protection Act) the verification of data processing carried out in the area of criminal justice by public prosecutors' offices. Nothing else can be inferred from the wording of § 32 Data Protection Act. The appellant further submits that it can be inferred from both Article 77 (1) GDPR and § 24 Data Protection Act that the Data Protection Authority may only deny concrete violations of data protection at the request of a data subject. No official action was provided for. However, the appellant is not successful with this argument: Pursuant to § 32 (1) (3) of the Data Protection Act, the Data Protection Authority must fulfil the tasks laid down in Article 57 (1) c to e, g, h and t of the GDPR in the area covered by § 36 (1) of the Data Protection Act with regard to the third main section. The provisions contained in this main body implement the Data Protection Directive, linking as far as possible to the provisions of the GDPR in order to avoid repetition and ensure a uniform level of protection (ErläutAB 2018 zu § 36 DSG). The Data Protection Authority therefore rightly assumed, in conclusion, that there is a power of official review under § 32(1) of the Data Protection Act in conjunction with Article 57(1)(h) of the GDPR. The assessment of the Data Protection Authority that the appellant has violated the right to secrecy pursuant to § 1 Data Protection Act by transmitting copies of files - to an extent exceeding that requested - to the accused and to an accident victim not specified by name, in that parts of files relating to proceedings concerning a traffic accident with physical injury resulting from negligence were transmitted to unauthorized third parties, cannot be contested.

Facebook-Entries and Freedom of Expression

The DSB - Data Protection Authority[17] dismissed the complaint about a "Facebook page of a municipality as the person responsible" and also ruled on media privilege within the meaning of § 9 (1) Data Protection Act respectively the "freedom of expression": The objected question was whether the respondent (an Austrian municipality) had infringed the complainant's (municipal council of the municipality) right to confidentiality by posting on its Facebook page on 7 November 2018 the list of participants in the "Zwischenpräsentation Parkraumkonzept E***stadt", on which the name of the complainant also appears, together with the comment

[17] DSB 18.12.2019, DSB-D123.768/0004-DSB/2019.

that the complainant did not attend this meeting. § 9 (1) Data Protection Act transposes the existing "media privilege" under data protection law under § 48 Data Protection Act 2000 into the GDPR system with an extended scope of application. The national provision in § 9 Data Protection Act ties in with Art. 85 GDPR, a fundamental provision including an opening clause. According to the express legal text of § 9 (1) of the Data Protection Act, two conditions must be cumulatively fulfilled in order to enter the privileged area of application: Firstly, personal data must be processed by media owners, publishers, media employees and employees of a media company or media service within the meaning of the Media Act (MedienG) and, secondly, such processing must be for journalistic purposes of the media company or media service. It should be noted that - despite the concerns about the restriction of the media privilege under § 9(1) Data Protection Act - a direct application of Art. 85(2) GDPR does not appear to be conducive to achieving the objective because of the primacy of Union law rules, since Art. 85(2) GDPR is not a substantive provision but - as mentioned above - contains a mandate to the Member States to enact corresponding legislation for specific processing situations. The analogous application of § 9 (1) Data Protection Act to the present case is also ruled out. It can therefore be assumed that only if the (strict) requirements of § 9 (1) Data Protection Act are met, legal protection is possible exclusively by way of the ordinary courts under the Media Act and that the Data Protection Authority has no jurisdiction. In all other cases, the Data Protection Authority is responsible for dealing with the content but has to take into account the right to freedom of expression under Article 11 EU GRC or Article 10 ECHR in the context of the balancing exercise. In the present case, as the operator of a publicly accessible Facebook profile, the respondent is to be qualified as the person responsible for data protection under Article 4(7) GDDPR, as it decides on purposes (sharing of content) and means (use of a publicly accessible Facebook profile). The respondent’s legitimate interests lie in freedom of expression in accordance with Article 10 ECHR and Article 11 EU-GRC, whereas the complainant's legitimate interests lie in the protection of his personal data in general and, furthermore, in protection against discrediting by the respondent. The complainant is a councilor in the municipality of E***stadt and thus a politician. It is clear that the respondent’s objective was to disseminate information to the public or, by publishing the list of participants, to initiate a contribution to a debate of general interest, namely whether the complainant, as a politician and public-interest person, fulfilled his tasks or requirements as a city councilor. The Data Protection Authority therefore comes to the conclusion that, on the basis of the weighing of interests carried out, there is no violation of the right to secrecy, since the legitimate interests of the respondent (freedom of expression) outweigh the stated impairments of the complainant's legitimate interests (secrecy with regard to the data subject of the proceedings) pursuant to § 1 (2) of the Data Protection Act.

Requests for Information in connection with an Identity and Credit Rating Database

The Federal Administrative Court[18] ruled on requests for information in connection with an identity and credit rating database: The complainant argued that the information provided by the operator of an identity and credit rating database remained incomplete with regard to the data processed: Categories of data, such as solvency and willingness to pay, which were specifically mentioned in the information, had not been provided. In summary, the Data Protection Authority explained to the Federal Administrative Court that the right to information under Art. 15 (1) lit. c GDPR had been met, since specific recipients as well as the purpose and context of the transmissions had been disclosed, so that it was now possible for the complainant to exercise his rights as a data subject directly vis-à-vis the two recipients as

[18] BVwG 09.12.2019, W214 2221970-1/15E.

persons responsible. A substantive right to information about the data actually processed could not be derived from Article 15(1)(c) GDPR; however, according to the Federal Administrative Court, this view cannot be accepted for the following reasons. In this regard, it should first be noted that it follows from Article 15, (1) GDPR that the data subject has a right of access to the personal data processed. In addition, the data subject (inter alia) has a right to be informed about the recipients or categories of recipients to whom the personal data have been or will be disclosed, in accordance with letter c. The Federal Administrative Court does not share the view of the relevant authority that these provisions should be read separately and that, accordingly, although the data subject has a right of access to the personal data processed and to the recipients or categories of recipients, the Federal Administrative Court does not share the view that the data subject has a right of access to the personal data transmitted to the recipients. This already follows from the wording of the provision and the legal system, according to which the data subject has "access to this (= the transmitted) personal data and to the following information "c) the recipients or categories of recipients to whom the (= those of paragraph 1) personal data have been or will be disclosed. Lit. c is to be read together with paragraph 1 because of its subordination to paragraph 1, and lit. c also refers to the personal data of paragraph 1 when referring to recipients to whom the personal data have been disclosed. The provisions of Article 15(1) and Article 15(1)(c) GDPR should therefore be read together, contrary to the view of the Data Protection Authority, so that it follows that there is also a right of access to the specific data transmitted to the recipients. As can be seen from the contents of the file, the relevant data were transmitted in 2018, for this reason alone it was to be assumed that the operator of the identity and credit rating database still stored the data. This was expressly confirmed by the operator of the identity and credit rating database, who also referred to § 152(2) of the 1994 GewO, according to which operators of credit agencies are obliged to keep their business correspondence and accounts for seven years. For the sake of completeness, it is noted that the data relating to the complainant, even if stored separately from the credit rating and identity database, are still personal and, since they are stored under the correspondence with the respective customers, can be easily found in the given case. The operator of the identity and credit rating database did not claim that the data could not be found, and such an objection would not be successful. The operator of the identity and credit rating database is therefore obliged to provide information on the content of the data transmitted by him to the recipients named in the ruling. In the absence of substantive special provisions in the Data Protection Act or in the GDPR, there is also no claim for reimbursement of legal fees under § 74 (2) AVG: Nor are there any indications that there is any loophole in the law that would allow it to be closed by analogy. On the contrary, the legislator expressly decided in favor of a general self-financing of costs in administrative proceedings and it cannot be assumed that it intended to regulate a claim for reimbursement of costs in the Data Protection Act and merely "forgot" to do so. Pursuant to Article 79 GDPR, the complainant could have enforced a claim for the violation of data protection before an ordinary court; in such disputed civil proceedings, a claim for costs exists in the event of victory.

Das Bundesverwaltungsgericht (30.10.2019, W258 2216873-I) sprach im Zusammenhang mit der Speicherdauer für Bonitätsdaten einer Kreditauskunftei aus, dass – unter Verweis auf die KapitaladäquanzVO der EU – ein historischer Beobachtungszeitraum von fünf Jahren angemessen sei, sodass – auch im Lichte der Regelungen zum Gewerbe der Kreditauskunftei (§ 152 GewO) - es zulässig sei, Insolvenzdaten auch nach deren Löschung aus der staatlichen Insolvenzdatei gespeichert bleiben dürfen. Im konkreten Fall hatte das zur Konsequenz, dass das Gericht es für angemessen hielt, dass Bonitätsdaten für einen Zeitraum des Insolvenzverfahrens (hier: sieben Jahre) plus weitere fünf Jahre (= 12 Jahre) gespeichert bleiben durften.

Pending Bills Supplementing the Austrian Data Protection Law

At the moment there are no pending bills supplementing the Austrian date protection law.

CUSTOMER TRACKING

Restrictions on the Use of Cookies

Section 96(3) of the Austrian Telecommunications Act (TKG 2003) stipulates that operators of public communications services and providers of digital services as defined in the E-Commerce Act are obliged to inform subscribers or users about the personal data[109] that the operator or provider will collect, process, and transmit, about the legal basis for those activities, about the purposes for which these activities will be carried out, and about the period of time for which these data will be stored.

Collecting these data will be permissible only upon the consent of the subscriber or user. This will not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over a communications network or as strictly necessary in order for the provider of a digital service explicitly requested by the subscriber or user to provide the service.

The subscriber will also be informed of the usage possibilities based on search functions embedded in electronic versions of the directories.

The information will be given in an appropriate form, in particular within the framework of general terms and conditions and, at the latest, upon commencement of the legal relations.

The right to information pursuant to the DSG will remain unaffected.

Other Forms of Tracking

The Austrian TKG does not specifically refer to cookies, but to “information stored on the device.”

DIRECT MARKETING AND COMMERCIAL COMMUNICATIONS

Applicable Austrian Laws

Several Austrian laws stipulate prohibitions of unsolicited commercial communications:

- TKG 2003: (Austrian) Federal Act 2003 enacting a Telecommunications Act and amending the Federal Act on Work Inspection in the Field of Transport and the KommAustria Act, original version in Federal Law Gazette 2003/70, amended by Federal Law Gazette I 2018/29.
- ECG: Federal Act that regulates certain legal aspects of electronic commercial and legal

[109] Compare however ECoJ October 1, 2019, C-673/17—Planet49.

transactions. (E-Commerce Act), original version in Federal Law Gazette I 2001/152, amended by Federal Law Gazette I 2015/34.

- UWG: Federal Act Against Unfair Competition of 1984, original version in Federal Law Gazette 1984/448, amended by Federal Law Gazette I 2016/99.

Telecommunications Act 2003 (TKG 2003)

Section 107 of TKG 2003 prohibits (i) calls including facsimile transmission and (ii) electronic mail when used for unsolicited commercial communication.

According to Section 92 TKG 2003, the provisions of the GDPR are to be applied to Chapter 12 of TKG. Therefore, according to GDPR Art. 6, an active consent is necessary for advertising calls and advertising e-mails.

Calls and Faxes

Calls, including facsimile transmissions, for marketing purposes are not permitted without the prior consent of the subscriber. The consent of the subscriber will be equivalent to the consent of a person authorized by the subscriber to use his line. However, the consent given can be withdrawn at any time; withdrawal of the consent must not have an impact on any contractual relationship with the addressee of the consent.

In this context the definition of “calls” in Section 92 TKG 2003 is of importance: a “call” is a connection established by means of a publicly available telephone service allowing two-way communication in real time.

Even when a consent is in place, in case of telephone calls for marketing purposes, the caller may not eliminate or falsify calling line identification, nor may the service operator be instructed to eliminate or falsify calling line presentation.

Electronic Mail

The definition of “electronic mail” under the TKG 2003 is significant: “any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.”[110]

Based on this definition, Section 107 of TKG 2003 reads for unsolicited electronic mail as follows: “The sending of electronic mail—including SMS messages—without the recipient's prior consent will not be permitted if (i) the sending takes place for purposes of direct marketing or (ii) is addressed to more than 50 recipients.”

Section 107(3) of TKG 2003 provides exceptions from the above-prerequisite of a “prior consent” regarding electronic mail for purposes of direct marketing:

Prior consent to electronic mail will not be required if:

- The sender has received the contact details for the communication in the context of a sale or a service to his customers;
- The communication is transmitted for the purpose of direct marketing of his own similar products or services;

[110]TKG 2003, Section 92.

- The recipient clearly and distinctly has been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use; or
- The recipient has not generally refused to receive such mail in the first place, especially by registering in the list named in Section 7(2) of the E-Commerce Act (ECG).

Furthermore, Section 107(5) of TKG 2003 includes a general clause that provides when electronic mail is prohibited—irrespective of the above exception:

> The sending of electronic communications for purposes of direct marketing will be prohibited in any case if:

- The identity of the sender on whose behalf the communication is transmitted is disguised or concealed;
- The provisions of Section 6(1) E-Commerce Act are violated;
- The recipient is asked to visit websites that violate that provision; or
- There is no valid address to which the recipient may send a request that such communications cease.

Regarding the international enforcement of the prohibitions of the use of electronic mail for purposes of direct marketing, Section 107(6) of TKG 2003 states: "If administrative offenses […] have not been committed in Austria, they will be considered as having been committed in the place where the unsolicited message reaches the subscriber's line." Therefore, the above applies also when electronic mail for purposes of direct marketing are sent to Austria from a foreign country.

E-Commerce Act (ECG)

Following the European Union e-Privacy Directive (2002/58/EC), Section 7 (Austrian) E-Commerce Act (ECG) stipulates *inter alia* the keeping of a "Robinson-list." The *Rundfunk und Telekom* communications by electronic mail. Information can be entered on the list free of charge.[112]

A service provider that sends a commercial communication by electronic mail without prior approval of the recipient must ensure that the commercial communication is identifiable clearly and unambiguously as such when received by the user. Furthermore, the service provider must ensure that the recipients are not on the "Robinson-list." However, whether a commercial communication by electronic mail without prior approval of the recipient is admissible has to be evaluated pursuant to the TKG 2003 discussed earlier in this chapter.

Federal Act Against Unfair Competition—UWG

The UWG prohibits unfair trade practices. The Austrian case law that pertains to the UWG has developed groups of patterns that are considered to be contrary to fair trade practices, for example, the negligent or intentional breach of the TKG, ECG, and/or DSG, to the extent that it leads to a competitive advantage, in order to advertise on an unnecessary personal level or

[112] *See* http://www.rtr.at/en/tk/E_Commerce_Gesetz.

in a pestering way (“psychological pressure to buy”), etc.

Under Austrian case law, some direct marketing methods are considered to be contrary to fair trade practices, e.g., fake personal post cards, use of illegally obtained customer data of competitors, etc.

An amendment of the Austrian Unfair Competition Act implemented Directive 2005/29/EC concerning Unfair Business-To-Consumer Commercial Practices in the Internal Market. It makes it illegal to, among other things:

- Conduct personal visits to the consumer's home, ignoring the consumer's request to leave or not to return except to enforce a contractual obligation;
- Make persistent and unwanted solicitations by telephone, fax, e-mail, or other remote media except in circumstances and to the extent justified to enforce a contractual obligation;
- Include in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them; or
- Explicitly notify a consumer that if he does not buy the product or service, the seller's job or livelihood will be in jeopardy.

Direct Marketing by Third Parties

Third parties have to meet the above legal requirements when conducting direct marketing actions. Whenever the direct marketing is conducted by electronic mail or by telephone, these third parties must have obtained the prior consent of the data subject/recipient as discussed in the prior sections.

ELECTRONIC COMMUNICATIONS

Applicable Austrian Laws

The two laws that define the primary regulations of electronic communications are:

- **TKG 2003:** Austrian Federal Act 2003 enacting a Telecommunications Act and amending the Federal Act on Work Inspection in the Field of Transport and the KommAustria Act, original version in Federal Law Gazette 2003/70, amended by Federal Law Gazette I 2018/29.
- **StGB:** Austrian Criminal Penal Act, original version in Federal Law Gazette 1982/205, amended by Federal Law Gazette I 2017/117.

What Is Prohibited

Both the StGB and the TKG 2003 safeguard the confidentiality of electronic communications in the broadest sense.

Section 93 of TKG 2003 stipulates that the content, traffic data, and location data are subject to confidentiality of the communications. Confidentiality of the communications also refers to information about unsuccessful connection attempts. Each operator and all persons who are involved in the operator's activities must observe confidentiality of the communications. The obligation to maintain confidentiality continues to exist also after

termination of the activities under which it was established.

Persons other than a user must not be permitted to listen, tape, record, intercept or monitor communications and the related traffic and location data as well as pass on related information without the consent of all users concerned. This provision does not apply to the recording and tracing of telephone calls when answering emergency calls and to cases of malicious call tracing, monitoring of communications, providing information on data in communications, and to technical storage that is necessary for the conveyance of a communication.

If communications are received unintentionally by means of a radio system, a telecommunications terminal equipment or any other technical equipment that is not intended for this radio system, this telecommunications terminal equipment, or the user of the other equipment, the contents of the communications as well as the fact that they have been received must neither be recorded nor communicated to unauthorized persons nor used for any purposes. Recorded communications must be erased or otherwise destroyed.

Editorial confidentiality (Section 31 Austrian Media Act) as well as further obligations of secrecy are to be respected in accordance with the protection of official secrecy of clergymen and of professional secrecy as well as the prohibition of circumventions thereof. The provider is not obliged to any corresponding examination.

Because it would go beyond the scope and length of this chapter, the most important matters of fact of the StGB in this context are just mentioned in an overview:

- Violation of the secrecy of the telecommunication;[113]
- Illegal interception of data;[114] and
- Misuse of data recorders and listening devices.[115]

Requirements

Pursuant to Section 96 of TKG 2003, master data, traffic data, location data, and content data may be collected and processed only for the purposes of providing the communications service. The transmission of these data may take place only to the extent necessary for the communications services for which these data have been collected and processed. The data may be used for marketing of communications services or the provision of value-added services as well as for other transmissions only with the consent of the data subjects. This consent may be withdrawn at any time. Such use must be restricted to the necessary extent and the period necessary for the marketing. The providers must not make the provision of their services dependent on such consent.

The operator must erase the master data at the latest upon termination of the contractual relations with the subscriber. Exceptions are permitted only to the extent to which the data is still required to settle or collect charges or handle complaints.[116]

Except for cases regulated by law, traffic data must not be stored and must be erased or

[113]StGB, Section 119.

[114]StGB, Section 119a.

[115]StGB, Section 120.

[116]TKG 2003, Section 97.

made anonymous after termination of the connection.[117]

In principle, content data must not be stored unless the storage of the data constitutes an essential component of the communications service. If short-term storage is required for technical reasons, the provider must immediately erase the stored data when the reasons cease to exist. The provider must make technical and organizational arrangements to ensure that content data is not stored or only to the minimum extent required for technical reasons. If storage of the content is a facility, the data must be erased directly after provision of the service.[118]

Location data other than traffic data may be processed only if they are (i) made anonymous or (ii) the users or subscribers have given their consent, which may be withdrawn at any time. Even in cases where the consent of the users or subscribers has been obtained for the processing of data, the user or subscriber must have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each transmission.[119]

Enforcement; Lawsuits; Penalties

Each operator and all persons who are involved in the operator's activities, who (i) without authorization discloses the fact or the contents of the telecommunications traffic of specific persons to an unauthorized person, or gives such person the opportunity to perceive facts himself that are subject to the obligation to maintain secrecy, and/or (ii) falsifies, incorrectly relates, modifies, suppresses or incorrectly conveys a communication, or withholds it from the intended recipient without authorization, may be punished by the criminal court with a prison sentence of up to three months or a fine of up to 180 times the daily rate.[120] Furthermore, the TKG 2003 stipulates administrative penalties for certain violations of the data protection regulations stipulated by the TKG 2003.

The following gives an overview of the possible penalties pursuant to the StGB, enforced by the Austrian penal courts:

- Violation of the secrecy of the telecommunication:[121] Imprisonment up to six months, or a fine of up to 360 times the daily rate.
- Illegal interception of data:[122] Imprisonment up to six months or a fine of up to 360 times the daily rate.
- Misuse of data recorders and listening devices:[123] Imprisonment up to one year or a fine of up to 360 times the daily rate.

Furthermore, the victim has the right to file actions for cease and desist (if there is the possibility that the violation could happen again) and compensation of the actual damages with

[117] TKG 2003, Section 99.

[118] TKG 2003, Section 101.

[119] TKG 2003, Section 102.

[120] TKG 2003, Section 108.

[121] StGB, Section 119.

[122] StGB, Section 119a.

[123] StGB, Section 120.

the Austrian civil courts. Section 1328a Austrian General Civil Code provides for the right of compensation regarding immaterial damage, if privacy was extensively violated and the victim was embarrassed in public.

EMPLOYEE INFORMATION

The protection of employee's personal information in the Austrian legal system is based on a combination of labor contractual, workers' constitutional, and data protection rules.

The rules do not cover identical fields and therefore general descriptions about the protection of employees' personal information are difficult, e.g., the employed Managing Director of an Austrian Ltd (GmbH) or Austrian Plc is not subject to the constitutional provisions that apply to employees. On the other hand, a freelancer could be subject to the constitutional provisions that apply to employees but not to the regulations regarding labor contracts, etc.

CHILDREN INFORMATION

Article 6 GDPR and Section 4, para. 4 DSG apply to the protection of children personal data. Generally, there are no specific rules applied to children information in Austria.

In the case of an offer of digital services that is made directly to a child, consent pursuant to Article 6/1/a GDPR for the processing of personal data of the child is legal if the child is at least 14 years of age.

VIDEO RECORDING

Video Recording in Private Spaces

The Federal Administrative Court[19] ruled that there is no room for the following Austrian special provisions on image processing (§§ 12 and 13 DSG) due to the lack of a corresponding “opening clause” in the GDPR and they must therefore not be applied. Nichtsdestotrotz sind nach Ansicht des Gerichts die allgemeinen Regeln der DSGVO anzuwenden. Für die Beurteilung eines datenschutzrechtlichen Verantwortlichen ist allein entscheidend, wer letztlich über die (Bild)Datenverarbeitung entscheidet, weshalb diese Verantwortlichkeit immer für sich allein und damit losgelöst von sonstigen allfälligen Auftragsverhältnissen zu beurteilen ist. [20]

Nevertheless, the following provisions are still in the act and therefore shown here:

Pursuant to the DSG,[124] “recording images” means observing occurrences in public or non-public space for private purposes, using technical devices for the processing of images. Recording images also includes acoustic information processed together with the images. This Part will apply to such recording of images unless other laws provide for more specific provisions.

[19] BVwG 18.12.2019, W211 2209492-1.

[20] BVwG 09.06.2020, W256 2224548-1.

[124] DSG Section 12.

Recording images is permitted if:

- (i) It is necessary in the vital interest of a person;
- (ii) The data subject has consented to the processing of the data subject's personal data;
- (iii) It is ordered or permitted by special statutory provisions, or
- (iv) There are overriding legitimate interests of the Controller or a third party in a particular case, and proportionality is given.

Recording images pursuant to (iv) above is permitted, in particular, if:

- It serves the precautionary protection of persons and items on private land exclusively used by the Controller and does not reach beyond the boundaries of the piece of land, except when it includes public traffic areas, which may be unavoidable to fulfil the purpose of the image recording;
- It is required for the precautionary protection of persons or items in publicly accessible places that are subject to the Controller's right to undisturbed possession because that right has already been infringed or because the place, by its nature, has a special risk potential, and no less restrictive appropriate measures are available, or
- It serves a private documentary interest and does not aim to record uninvolved persons to identify them or to record, in a targeted manner, items that are appropriate for indirectly identifying such persons.

It is not permitted to:

- Record images in a data subject's most private sphere without the express consent of the data subject;
- Record images to monitor employees;
- Align, in an automated manner, personal data obtained from image recordings with other personal data; or
- Analyse personal data obtained from image recordings on the basis of special categories of personal data (GDPR Art. 9) as selection criteria.

Except the recording serves a private documentary interest, the Controller must take appropriate measures corresponding to the risk posed by an interference and ensure that unauthorised persons cannot access or subsequently change the image recording. Except in the case of real-time surveillance, the Controller will keep logs of every processing operation.

The Controller must erase personal data recorded if they are no longer necessary in relation to the purposes for which they were collected and if there is no other statutory obligation to maintain the data. Maintaining data for more than 72 hours must be proportionate; separate logs of these data must be kept, and reasons must be stated.

Except the recording serves a private documentary interest, the Controller of an image recording must appropriately mark the recording. The warning sign must clearly specify the Controller, unless the Controller is already known to the data subjects based on the circumstances of the case. If, in violation of above, sufficient information is not provided, every data subject potentially affected by a processing operation can request information on the identity of the Controller from the owner of, or person authorised to use, the piece of land or building or other property from which the processing operation evidently originates. Failure to

provide such information without giving reasons will be deemed a refusal to provide access pursuant to GDPR Art. 15.

The Austrian Supreme Court[21] ruled: The household privilege of Art 2(2)(c) GDPR does not apply here: The material scope of application of the GDPR does not apply if the processing of personal data by natural persons is carried out for the sole purpose of carrying out personal or family activities (Art 2 (2) lit c GDPR). This privilege must be interpreted restrictively. In principle, private photo and video recordings are also covered by this exception and would therefore not be covered by the scope of the GDPR. However, as soon as a camera system is used not only for family purposes but also, for example, for the preservation of evidence, then this household privilege does not apply. § 12 Data Protection Act regulates the admissibility requirements for image acquisition. Only the admissibility criterion of § 12 (2) (4) Data Protection Act ("if in the individual case there are predominant legitimate interests of the person responsible or a third party and proportionality is given") could be applicable here.

WHISTLEBLOWING

There are no Austrian regulations that directly address the topic of “whistleblowing” or “whistleblowing hotlines.” However, due to the exterritorial effect of the U.S. Sarbanes-Oxley Act (SOX) on certain international and U.S. companies, there have been several decisions by the Austrian Data Protection Authority and even Guidelines for international/ groupwide Whistleblowing Systems (in German: https://www.dsb.gv.at/hinweisgebersystem):

- The Austrian subsidiary of an international group of companies is the Controller of such system;
- The right of the parent company to obtain relevant violations is limited to the ones by the top management of the (Austrian) subsidiary companies. Relevant violations are serious violations of business-relevant rules;
- The persons entrusted with the processing of whistleblowing messages are strictly separated from the everyday business. They must be especially trained and expressly obliged to the confidentiality of the reported data;
- The system may allow anonymous whistleblowing messages but does not encourage them. Rather, the system ensures full confidentiality regarding the identity of the whistle-blower;
- The accused person (members of the top management) will, in general, have access to the allegations;
- The identity of the whistle-blower may only be disclosed if it turns out that the allegation was deliberately false;
- In general, all data regarding the whistleblowing report are deleted within two months after the first message;
- Employees must be required to use the whistleblowing system;
- There must to be an intra-group contract that lays down the data protection obligations.

[21] OGH 27.11.2019, 6Ob150/19f.

DIRECTIVE (EU) 2017/680 IMPLEMENTATION

Austria has complied with the implementation of the Directive (EU) 2016/680 with the Data Protection Adaptation Act 2018.[125]

In addition to its function as supervisory authority under the DPA Regulation, the Data Protection Authority (DSB) has also been established as the competent supervisory authority under the EU DS Directive Criminal Law (Art. 31(1) DSG 2018). Furthermore, in addition to the implementation of this Directive with regard to law enforcement, data processing in other areas, such as national security, intelligence services and military self-security, are also covered by this third main section and the DSB is established as the competent Supervisory Authority. This deliberately includes data processing operations that do not fall within the scope of Union law.

NIS DIRECTIVE IMPLEMENTATION

In the end of 2018, Austria has complied the implementation of the Directive (EU) 2016/1148 with the Network and Information System Security Law (NISG).[126]

OTHER AUSTRIAN LAWS PROTECTING PERSONAL DATA

There are several hundred provisions in the Austrian legal system referring to the protection of personal data, for example:

- Acts regulating trade secrets (from December 2018 on new provisions in the Austrian Unfair Competition Act);
- Acts regulating the different professions and their chambers;
- Acts regulating the health sector and the use of medical data;
- Acts regulating the (social) insurances;
- Acts regulating the military and police forces;
- Acts regulating the different proceedings of elections;
- Acts regulating the societies and companies;
- Acts regulating post and infrastructure services;
- Acts regulating the court and administrative proceedings;
- Acts regulating the different elections;
- Acts regulating the possibility and obligation for statistics;

[125]BGBl. I Nr. 120/2017, *available at* https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig.

[126]BGBl. I Nr. 111/2018, *available at* https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_I_111/BGBLA_2018_I_111.pdfsig.

- Acts regulating the financial market;
- Acts regulating the use of personal data for the purpose of science and research; and
- Acts regulating the use of personal data in schools, high schools, and universities.

Depending on the actual matters of facts it is possible that several data protection regulations are applicable. The applicable regulations can only be evaluated case by case.

GEISTWERT
RECHTSANWÄLTE LAWYERS AVVOCATI

MMag.
JULIANE MESSNER
Partner

tel +43 1 585 03 03-20
fax +43 1 585 03 03-99
Linke Wienzeile 4
1060 Wien · Vienna · Austria
juliane.messner@geistwert.at
www.geistwert.at

GEISTWERT
RECHTSANWÄLTE LAWYERS AVVOCATI

Dr., LL.M. (IT-Law), LL.M.(Strathclyde)
MAX W. MOSING
Partner

tel +43 1 585 03 03-30
fax +43 1 585 03 03-99
Linke Wienzeile 4
1060 Wien · Vienna · Austria
max.mosing@geistwert.at
www.geistwert.at