PANORAMIC

DATA PROTECTION & PRIVACY

Austria

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: September 3, 2025

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Austria

Knyrim Trieb Rechtsanwälte

Rainer Knyrim ky@kt.at
Jennifer Salomon js@kt.at

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legislative framework for the protection of personally identifiable information (PII) in Austria mainly consists of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and the Data Protection Act (DPA), which implement the mandatory opening clauses and provisions of the GDPR. The DPA also enshrines the fundamental right to data protection at the constitutional level. Further, privacy-related provisions can be found in the following:

- the Telecommunications Act regarding electronic advertising and the processing of personal communication data of users by telecommunication service providers;
- the Act on Banking regarding banking secrecy;
- the Collective Labour Relations Act regarding data applications for the purposes of personnel administration and evaluation;
- the Trade Code 1994, especially regarding address publishers and direct marketing companies;
- the E-Commerce Act regarding certain aspects of electronic commercial and legal transactions;
- the Network and Information Systems Security Act regarding cybersecurity;
- the Electricity Act 2010 regarding organisations of the electricity sector;
- the Health Telematics Act 2012 (along with the Health Telematics Regulation and the Federal Electronic Health Record Regulation 2013) regarding technical data security measurements for the transmission of health data;
- the Research Organisation Act regulates data processing for research purposes by scientific institutions;
- Chapter 3 of the DPA, which implements Directive (EU) 2016/680 (the Law Enforcement Directive) and, together with the Security Police Act, regulates the processing of PII for purposes of the security police;
- the DPIA Whitelist (DSFA-AV) regarding processing activities that can be conducted without a data protection impact assessment (DPIA);
- the DPIA Blacklist (DSFA-V) regarding processing activities that always require a DPIA; and
- the Whistleblower Protection Act, which implements Directive (EU) 2019/1937.
- the Freedom of Information Act, which comes into force in September 2025.

Law stated - 22 Mai 2025

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Data Protection Authority (the Authority) safeguards data protection under the provisions of the GDPR and the DPA. The Authority also exercises its powers in relation to the highest governing bodies or officers referred to in article 19 of the Federal Constitutional Law and concerning the President of the National Council, the President of the Court of Auditors, the President of the Supreme Administrative Court and the Chairman of the Ombudsman Board in the area of the administrative matters to which they are entitled.

The Authority is established as a national supervisory authority under article 51 of the GDPR. The Authority acts as an authority supervising staff and as a human resource department.

Every data subject has the right to lodge a complaint with the Authority if they consider that the processing of their PII infringes the GDPR or section 1 of the DPA.

The Authority is responsible for imposing fines on natural and legal persons within the limits of its powers. Under section 11 of the DPA, the Authority will apply the catalogue of article 83(2)–(6) of the GDPR in such a way that proportionality is maintained. Under article 58 of the GDPR, the Authority makes use of its remedial powers, in particular by issuing warnings, especially in the event of initial infringements.

The DPA empowers the Authority with further powers in addition to the investigative powers under article 58 of the GDPR. The DPA can request from the controller or the processor of the examined processing all necessary clarifications and inspect data processing activities and relevant documents. The controller or processor shall render the necessary assistance. Supervisory activities are to be exercised in a way that least interferes with the rights of the controller or processor and third parties.

For the purposes of the inspection, the Authority will have the right, after having informed the owner of the premises and the controller or processor, to enter rooms where data processing operations are carried out, put data processing equipment into operation, carry out the processing operations to be examined and make copies of the storage media to the extent strictly necessary to exercise its supervisory powers.

In the case of a data processing operation causing serious immediate danger to the interests of confidentiality of the data subject that deserves protection (imminent danger), the Authority may prohibit the continuation of the data processing operation by an administrative decision under section 57(1) of the General Administrative Procedure Act 1991. The continuation may also be prohibited only partially if this seems technically possible, meaningful regarding the purpose of the data processing operation and sufficient to eliminate the danger. At the request of a data subject, the Authority can also order, by an administrative decision under section 57(1), the restriction of processing under article 18 of the GDPR if the controller does not comply with an obligation to that effect within the period specified. If prohibition is not complied with immediately, the Authority will proceed under article 83(5) of the GDPR.

Law stated - 22 Mai 2025

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The rules governing cooperation between the lead supervisory authority and the other supervisory authorities concerned are laid down in article 60 of the GDPR. Article 61 of the GDPR provides for mutual assistance between the supervisory authorities. Under article 62 of the GDPR, the supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other member states are involved. To contribute to the consistent application of the GDPR, article 63 of the GDPR establishes a consistency mechanism according to which the supervisory authorities shall cooperate with each other and, where relevant, with the European Commission, through the consistency mechanism as set out in article 2 of the GDPR. The Parliamentary Data Protection Committee is set up as a supervisory authority for the National Council, the Federal Council, the Court of Audit and the Ombudsman Board in matters of data protection and must coordinate with the Austrian Data Protection Authority.

Law stated - 22 Mai 2025

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Besides the penalty provisions under the GDPR, breaches of data protection regulations can lead to criminal or administrative penalties. The third chapter of the second main part of the DPA provides specifying regulations regarding the implementation of remedies, liability and penalties. The implementation of administrative fines provides, to a certain extent, the possibility to impose fines primarily on legal persons.

A controller may be sanctioned for a breach that falls within the scope of the GDPR if it could not have been unaware of the unlawfulness of its conduct, regardless of whether it was aware of the breach of the provisions of the GDPR. In the case of liability of a legal entity, it is also irrelevant that the breach was committed by its management body or that this body was aware of it. It should, therefore, always be noted that fines can be imposed on legal persons without requiring the conduct of the natural person responsible for the infringement to be established.

No fines may be imposed on public authorities, public entities or public bodies, such as bodies established in particular under public or private law, which act on a statutory basis.

The fines for violations are regulated in article 83 of the GDPR. According to section 63 of the DPA, whoever, to unlawfully enrich him or herself or a third party, or intending to damage another person's claim guaranteed according to section 1(1) of the DPA, deliberately uses PII that has been entrusted to or has become accessible to him or her solely because of his or her professional occupation, or that he or she has acquired illegally, for him or herself or makes such data available to another person or publishes such data despite

the data subject's interest in confidentiality, shall be punished by a court and be subject to imprisonment up to one year or a fine of up to €720, unless the offence is subject to more severe punishment under another provision.

Other provisions may be found in the Austrian Criminal Law, which contains rules for punishments in the case of violations concerning data (eg, intentionally altering or deleting data).

Unless the offence meets the elements of article 83 of the GDPR or is subject to a more severe punishment according to other administrative penal provisions, an administrative offence punishable by a fine of up to €50,000 is committed by anyone who (under section 62 of the DPA):

- intentionally and illegally gains access to data processing or maintains obviously illegal access;
- intentionally transmits PII in violation of the rules on confidentiality and, in particular, intentionally uses data entrusted to them under the provisions granting the use of PII for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or of address data to inform or interview data subjects for other purposes;
- intentionally acquires PII in the case of emergency under false pretences violating section 10 of the DPA;
- processes images contrary to the provisions of Chapter 1, Part 3 of the DPA; or
- refuses inspection under section 22(2) of the DPA.

Attempts shall be punishable.

The penalty for the forfeiture of data storage media and computer programs, as well as image transmission and recording devices, may be imposed if these items are connected with an administrative offence.

The Authority shall be responsible for imposing fines on natural and legal persons within the limits of its powers. Under section 11 of the DPA, the Authority will apply the catalogue of article 83(2)–(6) of the GDPR in such a way that proportionality is maintained. Under article 58 of the GDPR, the Authority will make use of its remedial powers, in particular by issuing warnings, especially in the event of initial infringements.

Law stated - 22 Mai 2025

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Pursuant to article 78(1) of the GDPR and section 27 of the DPA, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. In accordance with article 78(2) of the GDPR and section 26 of the DPA, each data subject shall have the right to an effective judicial remedy where the supervisory authority that is competent pursuant to articles 55 and 56 does not handle a complaint or does not inform the data subject within three months

on the progress or outcome of the complaint lodged pursuant to article 77. The Federal Administrative Court has jurisdiction over these complaints. In principle, an appeal to the Higher Administrative Court is also admissible against decisions of the Administrative Court within the framework of the Administrative Court Act (article 133(9) in conjunction with section 21 of the Administrative Court Act).

Law stated - 22 Mai 2025

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

As a consequence of the constitutional status of the right for the protection of personally identifiable information (PII), the data protection law is applicable in all sectors. No type of organisation is exempted. Both public authorities and private organisations must obey the rules imposed by data protection law. However, under section 30(5) of the Data Protection Act (DPA), no fines may be imposed on authorities, public law corporate bodies or public entities, in particular, entities established under public or private law, that act on a statutory basis.

Law stated - 22 Mai 2025

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Since each of these activities regularly leads to the electronic use of PII, the provisions of the EU General Data Protection Regulation (GDPR) and DPA are generally applicable in these matters. Areas such as telecommunication or electronic marketing are regulated by the Telecommunications Act and the E-Commerce Act. The Criminal Law includes specific rules for punishments, for example, in the case of intentionally breaching the secrecy of telecommunication or abusively intercepting transferred data. The right to contradict the transmission of personally addressed advertisement material is defined in section 151(11) of the Trade Regulation Act. Monitoring employees and appraising their performance is governed by the Collective Labour Relations Act, which, to the extent of the respective provisions, also forms part of Austrian data protection law. If the monitoring is carried out with AI, the AI Act is also applicable. The DPA regulates the permissibility of recording images and provides for special data security and labelling measures. The current provisions of the Austrian Data Protection Act (DSG) on image processing (section 13(3) and (5) DPA) are currently not applicable, as they do not comply with the GDPR due to the lack of an applicable opening clause.

Law stated - 22 Mai 2025

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

A specific Act exists for the transmission of health data among health service providers and the Austrian Electronic Health Record, but as regards the core regulations of data protection, this Act refers to the GDPR. The same is true for regulations on credit information: credit information databases are mentioned in a few Acts referring to data protection, which have incorporated general provisions to be applied to various areas connected to the processing of PII.

The E-Government Act provides regulations for Federal Identity Management to enable authorities to identify people uniquely in governmental proceedings. The Act also deals with aspects of data protection by defining an identity management system that prevents the possibility of merging PII across multiple authorities.

If smart meters are used for the supply of electricity or gas, the applicable Acts contain provisions for the protection of PII and grant customers the right to have their data accessed or transmitted via the internet (the Electricity Industry and Organisation Act 2010 and the Gas Industry Act 2011).

The Research Organisation Act establishes specific data protection regulations for scientific or historical research or statistical purposes.

Under the Collective Labour Relations Act, the implementation of control measures and technical systems for the control of employees provided that these measures affect human dignity, requires the consent of works councils to be legally valid.

The Whistleblower Protection Act serves to protect whistleblowers (ie, persons who, due to their professional connection to a legal entity, have obtained information about certain legal violations and reported them). Examples of such legal violations are cases of corruption, data protection violations and human rights violations.

Furthermore, there are special rules for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes pursuant to section 7 DPA; and section 8 DPA regulates the provision of addresses for notifying and interviewing data subjects.

The new section 9 DPA ('media privilege') also provides exemptions from the scope of application of the GDPR for the processing of personal data by media owners, publishers, media employees and employees of a media company or media service within the meaning of the Media Act, as well as by other persons who contribute journalistically to the content of a medium or the content of the communications of a media service in a media company or media service on the basis of a contract, for journalistic purposes of the media company or media service.

Law stated - 22 Mai 2025

PI formats

What categories and types of PI are covered by the law?

In general, all activities regarding wholly or partly automatically processed PII and processing other than by automated means of personal data that form part of a filing system or are intended to form part of a filing system are covered by the DPA.

Law stated - 22 Mai 2025

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The GDPR applies to the processing of PII in the context of activities of establishing a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not. The GDPR also applies to the processing of PII of data subjects who are in the European Union by a controller or processor not established in the European Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the European Union.

Section 3 of the DPA has been deleted; hence, there is no specific regulation beyond that of the GDPR.

Law stated - 22 Mai 2025

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The GDPR gives broad cover to the processing of PII; any type of processing such as collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction is covered by its provisions.

The controller shall be responsible for, and be able to demonstrate compliance with, the provisions and principles of the GDPR relating to the processing of PII. Where the processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject (article 28(1) of the GDPR). Processing by a processor shall be governed by a contract or other legal act under EU or EU member state law that is binding on the processor regarding the controller.

Two or more controllers who jointly determine the purposes and means of processing shall be joint controllers. They shall determine their respective responsibilities in an agreement in

a transparent manner. These relationships can be of a legal nature but also reflect factual circumstances.

Law stated - 22 Mai 2025

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Statutory provisions regarding the data subject's consent and legitimate purpose for the processing and transmission of personal identifiable information (PII) have been harmonised with the EU General Data Protection Regulation (GDPR) as set out in Chapter 2 'Principles' of the GDPR. The principle of lawfulness pursuant to article 5(1) lit a of the GDPR is based on the principle of prohibition with the reservation of permission of the GDPR. Accordingly, personal data may not be processed, unless there is permission in article 6(1) of the GDPR.

In the case of an offer of information society services directly to a child, consent to the processing of PII of a child under article 6(1)(a) of the GDPR shall be lawful where the child is at least 14 years old (section 4(4) of the Data Protection Act (DPA)).

The processing of PI pursuant to the Whistleblower Protection Act is permissible. The permissibility of processing personal data under this Act includes the processing of PI related to a report (section 8 of the Whistleblower Protection Act).

Law stated - 22 Mai 2025

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

Under article 9(1) of the GDPR, the processing of special categories of PII (information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) shall be prohibited, unless a condition as laid down in article 9(2) of the GDPR is met.

The Health Telematics Act 2012 provides special legal provisions for the electronic transfer of personal health data and genetic data.

Further, the DPA contains reworded provisions for special data processing activities adapted to meet the preconditions of the GDPR. The Austrian legislator reworded new provisions on image processing that cover every observation of events. This leads to an extended scope (eg, photographs shall also be covered). The Federal Administrative Court assumes that the provisions on image processing of the DPA are in breach of EU law due to the lack of opening clauses in the GDPR and are, therefore, not applicable.

Processing PII 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, pursuant to section 4(3) of the DPA:

- an explicit legal authorisation or obligation to process such data exists; 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 under article 6(1)(f) of the GDPR, and how the data is processed safeguards the interests of the data subject according to the GDPR and the DPA.

Law stated - 22 Mai 2025

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Under the provisions of the EU General Data Protection Regulation (GDPR), controllers are required to provide information to data subjects whose personally identifiable information (PII) is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language, at the time when personal data is obtained. If PII is collected directly from the data subject, the controller must provide information laid down in article 13 of the GDPR. If PII has not been obtained directly from the data subject, the controller must provide, in addition to the information listed in article 13 of the GDPR, the categories of PII concerned from which source the PII originates and, if applicable, whether it came from publicly accessible sources (article 14 of the GDPR). Information provided under articles 13 and 14 shall be provided free of charge.

Law stated - 22 Mai 2025

Exemptions from transparency obligations

When is notice not required?

The obligation to provide information shall not apply where and insofar as:

- the data subject already has the information;
- obtaining or disclosure of the personal data is expressly regulated by law;
- the provision of information to the data subject proves impossible or would involve a disproportionate effort, especially in the case of processing for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes; or
-

the personal data must remain confidential subject to an obligation of professional secrecy regulated by law.

In addition to the exceptions under articles 13 and 14 of the GDPR, the Second Data Protection Amendment Act 2018 regulates exceptions from the obligation to provide information within the framework of the laws concerning healthcare professionals.

As long as and to the extent that this is necessary to protect, in particular, the identity of a whistleblower to prevent attempts to prevent, undermine or delay information or follow-up measures based on information, the obligation to provide information shall not apply, in particular for the duration of administrative or judicial proceedings or investigative proceedings.

Law stated - 22 Mai 2025

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

The GDPR applies directly and there are no stricter rules for principles relating to the processing of PII as set down in the Data Protection Act (DPA). Therefore, PII must be accurate and kept up to date. Inaccurate or outdated data shall be deleted or amended, and data controllers are required to take 'every reasonable step' to comply with the principles outlined in the GDPR.

As long as and to the extent that this is necessary to protect, in particular, the identity of a whistleblower to prevent attempts to prevent, undermine or delay information or follow-up measures based on information, the principle of data accuracy shall not apply, in particular for the duration of administrative or judicial proceedings or investigative proceedings.

Law stated - 22 Mai 2025

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

According to article 5(1) lit c of the GDPR, data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Section 4(2) of the DPA permits the storage of data until the next periodic deletion date, if the data is deleted periodically due to technical or commercial circumstances. Specific storage periods can be found in the respective national material laws.

Law stated - 22 Mai 2025

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) of the GDPR, subject to the implementation of the appropriate technical and organisational measures required by this Regulation to safeguard the rights and freedoms of the data subject. To meet the documentation requirements, retention periods must be defined and documented.

As long as and to the extent that this is necessary to protect, in particular, the identity of a whistleblower to prevent attempts to prevent, undermine or delay information or follow-up measures based on information, the principle of data retention shall not apply, in particular for the duration of administrative or judicial proceedings or investigative proceedings. Personal information that is not required for the processing of a report may not be collected or must be deleted immediately if it is collected unintentionally.

Law stated - 22 Mai 2025

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

According to article 5(1) lit b of the GDPR, data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The purpose limitation principle contributes to transparency, legal certainty and predictability and aims to protect the data subject by setting limits on how the controller may use their data. The controller must determine the purposes of the processing in advance, but no later than at the time the data is collected (or obtained). Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with article 89(1), not be considered to be incompatible with the initial purposes.

The DPA generally does not permit the processing of PII for purposes other than those for which the PII was originally collected. However, there are exceptions as follows:

- Article 5(1) lit b of the GDPR states that data may not be further processed in a manner incompatible with the specified purposes. Conversely, the strict principle of purpose limitation is thus broken insofar as further processing for compatible purposes is expressly permitted.
- Under section 7 of the DPA, PII may be further used for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- The Research Organisation Act also specifies more detailed provisions for the processing of PII for research purposes by scientific institutions.

Law stated - 22 Mai 2025

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

According to article 22(1) of the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or that significantly affect him or her. The use of automated processing can already constitute a decision within the meaning of article 22 GDPR if the result is 'relevant' for a specific – further – decision. Precise and extensive factual findings are required to prove the lack of 'relevance'.

Pursuant to article 13(2) lit f and article 14(2) lit g of the GDPR, information must be provided about the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The prohibition shall not apply if the decision is:

- necessary for the entering into, or the performance of, a contract;
- legally permissible on the basis of legal provisions; or
- based on explicit consent.

To compensate for this, the controller must take appropriate protective measures (article 22(3)). According to article 22(4) of the GDPR, sensitive data may only be used for an automated decision if there is a legal basis or explicit consent. Data relevant to criminal convictions and offences as defined in article 10 are not covered by this restriction. Permissible processing for an automated decision in an individual case is, however, reduced to those cases in which there is an authorisation according to section 4(3) of the DPA.

According to Recital 71, children should never be affected by automated decisions. However, not even the article 29 Working Party assumes an absolute prohibition, but urgently recommends making use of the exceptions of article 22(2)of the GDPR only in the interest of children (eg, safeguarding the best interests of the child) and thus to subject them to automated decisions in individual cases.

A decision of the Supreme Administrative Court (VwGH) of 21 December 2023 (Ro 2021/04/0010-11) deals with the processing of personal data of job seekers for their classification for reintegration into the labour market in the course of the Labour Market Opportunities Assistance System (AMAS) by the Public Employment Centre (AMS). AMAS is a computerised model for improving AMS counselling. The model proposes the categorisation of AMS customers into groups with high, medium and low labour market opportunities. Of particular interest are the statements of the VwGH on the existence of automated decision-making within the meaning of article 22 GDPR, taking into account the recent case law of the ECJ of 7 December 2023, C-634/21, SCHUFA Holding [Scoring]. In the opinion of the VwGH, based on the ECJ case law on SCHUFA scoring cited above, the profiling may constitute an automated decision in individual cases. The determination of the value of the probability of integration into the labour market is, therefore, already an 'automated decision' within the meaning of article 22(1) GDPR, as long as this value significantly determines the allocation to the intended customer groups and has a legal effect on the jobseekers. The VwGH, therefore, considers the view of the Federal Administrative Court (BVwG) to be incorrect, according to which the determination of the probability value

is only to be regarded as a preparatory action and the final decision on the allocation is the responsibility of the AMS advisers. Furthermore, according to the VwGH, the legal act, the Labour Market Service Act, does not contain any provision that would fulfil the justification criteria of article 22(2) lit b GDPR with regard to case-related processing. However, the existence of such an element would be necessary if automated processing would significantly influence the decision of the consultant at the AMS. It is now up to the BVwG to determine this.

On the basis of a recent ECJ decision (C-203/22 – Dun & Bradstreet), the data protection authority issued a newsletter informing that the data subject has the right to information in accordance with article 15(2)(h) GDPR about the procedure and the principles that were applied in the automated processing to obtain a certain result – for example, a credit profile. The specific algorithm does not necessarily have to be disclosed and will generally not be sufficiently comprehensible.

Law stated - 22 Mai 2025

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Data Protection Act (DPA) does not require any other or stricter obligations for the security of processing than those set out in the EU General Data Protection Regulation (GDPR). Additionally, there are further provisions for image processing regarding specific data security measures and labelling. Besides the duty of the controller using image processing to disclose it appropriately, it must be ensured that the access and manipulation of records by unauthorised persons are excluded. Any use of image processing must be documented; this does not apply to real-time observation. The Federal Administrative Court assumes that the provisions on image processing of the DPA are in breach of EU law due to the lack of opening clauses in the GDPR and are, therefore, not applicable.

Where a type of processing – in particular, processing using new technologies and taking into account the nature, scope, context and purpose of the processing – is likely to result in a high risk to the rights and freedoms of the natural persons, the controller shall carry out a data protection impact assessment.

According to clause 14 of the Standard Contractual Clauses, the controller shall carry out a data transfer impact assessment for third-country transfers.

Some of the material laws provide for specific data protection security obligations (eg, the Research Organisation Act, the Health Telematics Act 2012, the AI Act and the Whistleblower Protection Act).

Law stated - 22 Mai 2025

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Immediately after recognising a data breach, the controller should not only attempt to contain the incident but also assess the risk that could result from it. According to article 33 of the GDPR, in the case of a personal data breach, the controller shall, without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach of the Data Protection Authority via email, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

As long as and to the extent that this is necessary to protect, in particular, the identity of a whistleblower to prevent attempts to prevent, undermine or delay information or follow-up measures based on information, the right to be notified of a personal data breach shall not apply, in particular for the duration of administrative or judicial proceedings or investigative proceedings.

Law stated - 22 Mai 2025

INTERNAL CONTROLS

Accountability
Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

According to article 5(2) of the EU General Data Protection Regulation (GDPR), the controller must be able to demonstrate compliance with the data protection principles in article 5(1) of the GDPR, and according to article 24(2), the controller must be able to prove that the processing is carried out in accordance with the GDPR. This obligation is also reflected in the obligation to maintain a record of processing (article 30 of the GDPR). In more complex organisations, the implementation of the requirements of the GDPR, and article 24 in particular, can only succeed through a systematically structured data protection management system. Such a data protection management system should be implemented throughout the entire organisation, starting at the management level.

Law stated - 22 Mai 2025

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The designation of a data protection officer (DPO) is mandatory under the conditions of article 37 of the GDPR. The legislature has chosen not to provide a description of the criteria that a person must satisfy to act as a DPO. However, the required level of expertise is apparently based on the data processing operations carried out by the controller or processor and the protection required for the relevant data.

The obligations of the DPO are laid down in section 5 of the Data Protection Act (DPA). Without prejudice to other obligations of confidentiality, DPOs and persons working for the DPO shall be bound by confidentiality when fulfilling their duties. This shall apply in particular concerning 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 persons working for the DPO may exclusively use the information made available to fulfil their duties and shall be bound by confidentiality even after the end of their activities.

Section 5 of the DPA provides for rules on the right of the DPO and persons working for the DPO to refuse to give evidence. Within the scope of the DPO's right to refuse to give evidence, their files and other documents are subject to a ban on seizure and confiscation.

Public-sector DPOs 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 shall only comply with this to the extent that this does not contradict the independence of the DPO within the meaning of article 38(3) of the GDPR. Public-sector DPOs shall regularly exchange information, particularly regarding ensuring uniform data protection standards.

Considering the type and scope of data processing activities and depending on the facilities of a federal ministry, one or several DPOs shall be appointed in the sphere of responsibilities of each federal ministry. These DPOs shall be employed by the relevant federal ministry or the relevant subordinate office or other entity.

Law stated - 22 Mai 2025

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

To demonstrate compliance with the GDPR, the controller or processor should maintain records of processing activities under their responsibility (article 30 of the GDPR). Each controller and processor shall be obliged to cooperate with the supervisory authority and make those records available to the authority upon request.

Law stated - 22 Mai 2025

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Where a type of processing – in particular, processing using new technologies and taking into account the nature, scope, context and purpose of the processing – is likely to result in a high risk to the rights and freedoms of the natural persons, the controller must carry out a data protection impact assessment (article 35 of the GDPR). The purpose of this assessment is to describe the processing, to assess its necessity and proportionality, and to better control the risks to the rights and freedoms of natural persons and identify appropriate measures to address those risks. It obliges controllers to review their own data processing operations pursuant to articles 24, 25 and 32 and, where appropriate, to take specific (documented) protective measures to capture these risks and, in this way, to manage them appropriately. A 'threshold analysis' is required to identify those data processing operations that shall be subject to a data protection impact assessment. To clarify which processing operation shall be subject to a data protection impact assessment in any case, the supervisory authority established a list of the kind of processing operations (the blacklist). In addition, the supervisory authority also established a list of the kind of processing operations for which no data protection impact assessment is required (the whitelist).

Austrian legislation has made use of the opening clause of article 35(10) of the GDPR regarding certain legal provisions of national material laws and has carried out a data protection impact assessment as part of a general impact assessment in the context of the adoption of that legal provision (eg, the Research Organisation Act and the Whistleblower Protection Act).

The European Court of Justice's judgment in Case C-311/18 (***Schrems II***) recalled that protection for personal data must also be guaranteed wherever the data is transferred. The transfer must not result in the applicable level of protection falling below that guaranteed in the EEA. Therefore, transfer instruments, according to article 46 of the GDPR, must be used. In addition, the legal situation in the third country must be assessed to ensure that the transfer instruments actually ensure an adequate level of data protection.

Furthermore, it may be necessary to establish additional measures that are required to achieve this level of protection. According to clause 14 of the Standard Contractual Clauses, this assessment must be served by a datatransfer impact assessment, which must be made available to the competent supervisory authorities upon request.

Law stated - 22 Mai 2025

Design of PI processing systems
Are there any obligations in relation to how PI processing systems must be designed?

Pursuant to article 25(1) of the GDPR, the controller shall implement appropriate technical and organisational measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons. These measures shall be designed to effectively implement the principles of data protection, such as data minimisation, and to integrate the necessary safeguards into the processing to meet the requirements of the Regulation and to protect the rights of data subjects. Article

25 specifies the obligation of the controller, as set out in article 24, to ensure that personal data are processed in accordance with the GDPR by means of technical and organisational measures and already applies these measures at the 'point in time when the means are determined'. Article 25(1) deals with the principle of data protection by design and article 25(2) addresses the principle of data protection by default. According to article 25(3), an approved certification mechanism, pursuant to article 42, may be used as an element to demonstrate compliance with the requirements of article 25(1) and (2). The DPA does not alter the provisions of the GDPR, but Austrian legislation has made use of the opening clause of article 35(10) of the GDPR regarding certain legal provisions of national material laws and has carried out a data protection impact assessment as part of a general impact assessment in the context of the adoption of that legal provision (eg, the Research Organisation Act and the Whistleblower Protection Act).

Law stated - 22 Mai 2025

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no registration requirement and therefore no penalties.

Law stated - 22 Mai 2025

Other transparency duties

Are there any other public transparency duties?

Regarding the processing of images, section 13(5) of the Data Protection Act stipulates a special obligation of disclosure. The Federal Administrative Court assumes that the provisions on image processing of the DPA are in breach of EU law due to the lack of opening clauses in the EU General Data Protection Regulation and are, therefore, not applicable.

Law stated - 22 Mai 2025

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The rules regarding data processors, joint controllers and third parties under the EU General Data Protection Regulation (GDPR) apply directly without distinctions:

- if there is a processor pursuant to article 28 of the GDPR, a data processing agreement shall be concluded between the controller and the processor pursuant to article 28(3);

- if the service provider and the controller jointly determine the purposes and means of processing, they shall be joint controllers. Therefore, a joint controller agreement must be concluded in accordance with article 26 of the GDPR. The essence of the arrangement shall be made available to the data subject; and
- if the service provider acts as controller and there is no joint controllership, the transfer of personal information (PI) shall be based on a proper legal basis pursuant to article 6 of the GDPR.

Law stated - 22 Mai 2025

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The provisions of the GDPR apply directly. Specific restrictions concerning the disclosure of personal identifiable information can be found in particular national laws (eg, the Research Organisation Act).

Law stated - 22 Mai 2025

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The provisions of the GDPR apply directly. Under the provisions of the GDPR, international data transfer outside of the European Union is similar to the existing regime under Directive 95/46/EC (the Data Protection Directive). Data can be transferred to a third country or an international organisation only if the conditions laid down in Chapter V of the GDPR are complied with by the controller and processor, including onward transfers. A transfer of personal data to a third country or an international organisation may take place under a European Commission adequacy decision or other transfer safeguards under article 46 et seq of the GDPR (eg, standard contractual clauses, binding corporate rules or the explicit consent of the data subject).

Due to the Court of Justice of the European Union decision in ***Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*** (Case C-311/18) (***Schrems II***), in cases where standard contractual clauses are put in place, the legal situation in the data recipient's country must be examined up front (data transfer impact assessment). If no appropriate data protection legislation exists, additional technical and organisational measures must be adopted. On 10 July 2023, the European Commission adopted the adequacy decision on the EU-US Data Privacy Framework (EU-US DPF). The EU-US DPF provides a comparatively simple way to transfer personal data to the US, but only to those US companies that are listed on the official EU-US DPF list with a certification marked as 'active'.

Law stated - 22 Mai 2025

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Restrictions on data transfers outside the European Union also apply to transfers to service providers and onward transfers pursuant to Chapter V of the GDPR. The GDPR applies directly and there are no stricter rules set down in the Data Protection Act.

Law stated - 22 Mai 2025

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

For some processing operations that are carried out in fulfilment of a legal obligation, the retention period results directly from the law. More often, legal provisions have an indirect effect on the determination of the retention period, such as obligations to provide evidence and limitation periods for legal claims that can potentially be asserted against the controller. There is no specific regulation that requires PI or a copy of PI to be retained when transmitted or accessed from outside the jurisdiction.

Law stated - 22 Mai 2025

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

The right to access data is part of the rights of data subjects in connection with transparency. The EU General Data Protection Regulation (GDPR) stipulates that information must be provided where personally identifiable information (PII) is collected from the data subject. Under section 4(5) of the Data Protection Act (DPA), the right to access under article 15 of the GDPR does not apply to a controller acting on a statutory basis, without prejudice to other legal restrictions, if the provision of such access jeopardises the performance of a task assigned to the controller by law. Further, the right to access under article 15 of the GDPR does generally not apply to a controller, without prejudice to other legal restrictions, if the disclosure of such information would endanger a business or trade secret of the controller or third parties (section 4(6) of the DPA). At first glance, the ECJ came to the conclusion in an Austrian preliminary ruling procedure (C-203/22, Dun & Bradstreet Austria) that the exemption provision of section 4(6) DPA was incompatible with the GDPR because it did not allow the data protection authority to assess the balance of interests. However, the ECJ initially misrepresented section 4(6) DPA (despite the correct submission by the Vienna Administrative Court) and, in addition, both the referring court and the ECJ overlooked another relevant national provision (section 25(3) DPA). However, the practical effects of

these misunderstandings will be limited due to the similarity of the ECJ's findings with the actual wording of section 4(6) DPA in conjunction with section 25(3) DPA.

As long as and to the extent that this is necessary to protect, in particular, the identity of a whistleblower to prevent attempts to prevent, undermine or delay information or follow-up measures based on information, the right of access to information shall not apply for the duration of administrative or judicial proceedings or investigative proceedings (section 8(7) of the Whistleblower Protection Act).

Law stated - 22 Mai 2025

Other rights

Do individuals have other substantive rights?

Besides the right of access, data subjects have the right to request from the controller rectification or erasure of PII or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them, which is based on subparagraphs (e) or (f) of article 6(1), including profiling based on those provisions. Further, data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or that significantly affects them.

Law stated - 22 Mai 2025

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The GDPR allows data subjects to act against data protection violations, in addition to any imposed administrative fines under the GDPR. The subject may address civil courts to receive compensation for any material or non-material damage suffered as a result of a GDPR infringement. The DPA also provides a choice of the competent court in whose jurisdiction the place of domicile of the data subject and the seat of the defendant is situated and stipulates that the general provisions of civil law apply to the claim for damages in detail. The Court of Justice of the European Union confirmed that there is no 'threshold' for GDPR damages. Mere infringement of the GDPR does not give rise to a right to compensation. However, there is no requirement for the non-material damage suffered to reach a certain threshold of seriousness to confer a right to compensation. In addition, even the loss of control can constitute damage for which compensation can be claimed.

Austrian court decisions

The regional court of Wiener Neustadt ordered the city of Baden to pay damages of €500 due to a data leak, although the court found that there had been no theft or misuse of the data. Nevertheless, the fear and concern of possible misuse of the data alone justified

compensation. The court thus complied with the decision of the ECJ of 14 December 2023 (C-767/21), according to which companies and authorities are obliged to pay compensation in the event of data leaks, even if no demonstrable material damage has occurred.

In the decision 7 Ob 25/23m of the Supreme Court (OGH) on legal protection cover for immaterial damages from data protection violations, the Supreme Court came to the conclusion that the assertion of these damages is possible with legal protection insurance and is covered by general contract legal protection.

Law stated - 22 Mai 2025

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Every data subject has the right to lodge a complaint with the Data Protection Authority (the Authority) if the data subject believes that the processing of PII infringes the GDPR or the DPA. The Federal Administrative Court shall decide through a panel of judges on complaints against administrative decisions of the Authority. Further, each data subject can apply to the Federal Administrative Court if the Authority does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged.

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to article 77 of the GDPR, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. Therefore, a data subject may also file claims directly with the civil courts on the basis of article 79 of the GDPR.

Under the DPA, data subjects are entitled to mandate a non-profit-organisation body, organisation or association that has been properly constituted and has statutory objectives that are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms regarding the protection of their PII to lodge the complaint on his or her behalf and to exercise the rights referred to in sections 24 to 27 of the DPA. On the other hand, the DPA does not provide the opportunity to assign specialised organisations (data protection non-governmental organisations) to file claims for damages with the responsible civil court.

Under section 29(2) of the DPA, the Regional Court of First Instance has jurisdiction over the claim for damages, irrespective of the amount in dispute, which also results in an absolute obligation to be represented by a lawyer. The appointment of a senate (one chairman and two members) to decide on the claim can be requested by both the claimant (in the claim) and the defendant (in the defence) from an amount in dispute exceeding €100,000 under section 7a(1) of the Austrian Jurisdictional Standards. In the case of disputes between employers and employees in connection with the employment relationship, for example, in the case of the processing of personal data of employees by the employer, the labour and social courts have jurisdiction under section 3 of the Labour and Social Courts Act (the ASGG) in connection with section 50(1)(1) of the ASGG. In cases of public liability (ie, claims for damages against the federal government, provinces, districts, municipalities, other public corporations and the social insurance institutions), the regional court also has jurisdiction under section 9 of the Public Liability Act.

Law stated - 22 Mai 2025

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Section 9 of the Data Protection Act (DPA) implements the opening clause provided by article 85 of the EU General Data Protection Regulation (GDPR). The processing of personally identifiable information (PII) by media owners, editors, copy editors and employees of a media undertaking or media service within the meaning of the Media Act, for journalistic purposes of the media undertaking or media service, the provisions of the DPA and Chapters 2, 3, 4, 5, 6, 7 and 9 of the GDPR shall not apply. When exercising its powers towards the persons named in the first sentence, the Data Protection Authority must observe the protection of editorial confidentiality (section 31 of the Austrian Media Act). However, the Austrian Constitutional Court (VfGH) annulled this provision, as it contradicts the fundamental right to data protection. The fundamental right to data protection does not permit categorical priority of freedom of expression over the protection of personal data. Within the repair period until 30 June 2024, the legislator must now ensure a differentiated balance between the fundamental rights to data protection and freedom of expression. The repair of the 'media privilege' obtained by the VfGH is currently pending in the Austrian National Council.

Law stated - 22 Mai 2025

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

These issues must be evaluated under general principles and according to the provisions of the EU General Data Protection Regulation (GDPR) and the Telecommunications Act, respectively. Since Directive 2002/58/EC (the ePrivacy Directive) was amended by Directive 2009/136/EC (the Citizen's Rights Directive), new special regulations for the declaration of consent for the use of cookies on websites had to be translated to the Telecommunications Act.

Austria implemented the EU ePrivacy Directive in November 2011 and has simply translated article 5(3) of the Directive into section 96(3) of the Telecommunications Act. This provision has been transferred to section 165(3) of the Telecommunications Act 2020. Providers of an information society service are obliged to inform the user which personal information they will process, on what legal basis and for what purposes this will be done and for how long the data will be stored. The collection of this data is only permissible if the user has given their consent. This shall not prevent technical storage or access if this is strictly necessary for the provider of an information society service expressly requested by the user to be able to provide that service. The Telecommunications Act explicitly only refers to personal

cookies. The regulation is, therefore, contrary to EU law, as the regulation should also cover non-personal data.

Law stated - 22 Mai 2025

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Both the Telecommunications Act and the e-Commerce Act contain provisions for commercial communications and sanctions for cold calling and unsolicited faxes and emails. Commercial calls and the transmission of commercial messages are only legitimate with the recipient's prior consent. Some exceptions exist for the transmission of emails. Violating these provisions could lead to a fine of up to €37,000 for each unlawful email or up to €58,000 for each cold call, respectively.

Law stated - 22 Mai 2025

Targeted advertising

Are there any rules on targeted online advertising?

If targeted advertising is used as automated data processing (including profiling) within the meaning of article 22 of the GDPR in such a way that a data subject is subject to a decision based solely on automated data processing that produces legal effects concerning them or that significantly affects them, the legal consequences of article 22 of the GDPR apply. In advertising, profiling, pursuant to article 4 No. 4 of the GDPR, is commonly used, but automated decision-making, including profiling as defined in article 22 of the GDPR, is used less frequently. Calls and electronic mail for the purposes of direct advertising are not permitted without the user's prior consent in accordance with section 174 Telecommunications Act. An exception only exists for electronic mail in an ongoing customer relationship if there is a connection to products or services bought earlier by the customer.

Analog unaddressed mailing may only be delivered if delivery is not refused by means of an advertising waiver sticker on the mailbox or a written refusal of delivery. Therefore, the Robinson List of the Austrian Economic Chamber must be checked. In the case of addresses purchased from address publishers or direct marketing companies, section 151 Trade Regulation Act applies. This authorises address publishers and direct marketing companies to collect and use data from several sources.

Law stated - 22 Mai 2025

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

Under article 9(1) of the GDPR, processing of special categories of personal identifiable information (PII) (information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) shall be prohibited, unless a condition laid down in article 9(2) of the GDPR is met. Processing PII 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, pursuant to section 4(3) of the Data Protection Act (DPA):

- an explicit legal authorisation or obligation to process such data exists; 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 under article 6(1)(f) of the GDPR, and how the data is processed safeguards the interests of the data subject according to the GDPR and the DPA.

Law stated - 22 Mai 2025

Profiling

Are there any rules regarding individual profiling?

Profiling is merely a particular manifestation of automated processing. Article 22(1) contains a prohibition on subjecting a data subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or that significantly affects them. The term 'decision' is to be understood broadly and includes measures. According to article 4(4), profiling means any form of automated processing of personal data that consists in using personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Law stated - 22 Mai 2025

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The DPA does not contain specific rules regarding the use of cloud computing services. Hence, the general provisions of the GDPR are applicable. As cloud service providers are often located outside the European Economic Area, international data transfer needs special attention. If personal data is transferred to a third country in the context of cloud computing services, the provisions of Chapter V of the GDPR must be taken into account and a suitable transfer instrument must be selected in accordance with article 44 et seq of the GDPR. Other regulations may also be relevant depending on the industry, such as the Digital

Operational Resilience Act (DORA) or the NIS 2 Directive. The NIS 2 Directive has not yet been implemented in Austria.

According to the Health Telematics Act 2012, it must be ensured that health data is saved in storage that is provided based on the needs of clients (cloud computing) only if the health data has been encrypted using state-of-the-art technology (section 6(1), No. 2 of the Health Telematics Act 2012).

Law stated - 22 Mai 2025

UPDATE AND TRENDS

Key developments of the past year
Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Date Protection Act was amended twice in 2024, with a Supreme Court ruling being the decisive factor for both amendments.

First, the media privilege under section 9 of the Austrian Data Protection Act (DSG) was repealed. With the amendment to Federal Law Gazette I No. 62/2024, Section 9 paragraph 1 DSG was amended and paragraph 1a was added at the same time.

Furthermore, the amendment to Federal Law Gazette I No. 70/2024 established a separate data protection authority for the National Council, the Federal Council, the Court of Audit and the Ombudsman Board, including their administrative activities, in sections 35a ff DSG: the Parliamentary Data Protection Committee.

The first obligations of the AI Act came into force in February 2025. However, there are no special features for Austria here. The Rundfunk und Telekom Regulierungs is the responsible AI service agency in Austria.

Law stated - 22 Mai 2025