3 National Reports

1 Austria

Johann Cas, Felix Schaber (OEAW/ITA)

1.1 Informed consent

1.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Datenschutzgesetz (DSG)	https://anon.to/ggRI5X	Hard law with § 1 in the rank of a constitutional law	Enshrines the fundamental right to the protection of personal data with particular regard to the right to private and family life
Sicherheitspolizeigesetz (SPG)	https://anon.to/ZC9cb7 (German)	Hard law	Among other things regulates the use of personal data for police purposes
Polizeiliches Staatsschutzgesetz (PStSG)	https://anon.to/as6TeZ (German)	Hard law	Contains provisions for state security in addition to the norms found in the SPG
Forschungsorganisationsgesetz (FOG)	https://anon.to/u3P8mz (German)	Hard law	Contains specific provisions for processing personal data for research purposes

Main regulatory tools addressing data protection issues and informed consent in Austria

(vi) The GDRP does not apply to purely personal or household activity. Is there any provision under Austrian national law for the protection of these data categories?

Yes, the fundamental right to privacy enshrined in § 1 DSG does not contain an exception for personal or household activities. It is however limited to personal data with a legitimate interest worthy of protection.

(vii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

For security and cybersecurity, the main regulatory tools are the "Sicherheitspolizeigesetz" (SPG) and the "Polizeiliches Staatsschutzgesetz" (PStSG). The SPG regulates the usage of personal data for police purposes while the PStSG contains additional provisions for the purposes of state security.

While the DSG is still applicable, the SPG contains additional legal grounds for the processing of personal data. Legal grounds like defence against "criminal association" or "probable attacks against live, health, decency, freedom, property or environment" are rather broad and leave room for interpretation (§ 53 Abs 1 SPG). Police is also allowed to use video and audio recordings for such purposes (§54 Abs 4 SPG). However, the need to maintain the principle of proportionality and therefore choose the least invasive measure fit for the purpose (§ 29 Abs 2 SPG). Preventive measures against cyberattacks is within the Domain of the PStSG.

Name of Authority	Link	Is this an independent body?	Number of employees
Datenschutzbehörde	https://anon.to/y8sxJy	Yes	30

(viii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

No, the term is used but not defined in the Austrian DSG. However, the Austrian FOG which is designed to regulate data processing for research purposes defines the term "activities in research and experimental development" ("Tätigkeiten der Forschung und experimentellen Entwicklung") in § 2b Z 10 FOG. It characterizes these activities to be "novel, inventive, of uncertain end result, systematic and transferable and reproducible".

(ix) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

Yes, Art 89 GDPR is mainly implemented by the Austrian FOG with regards to research purposes. It contains provisions for "scientific institutions" ("wissenschaftliche Einrichtungen") when conducting activities in research. The term "scientific institution" is defined broadly and may be interpreted to include commercial research in companies (§ 2b Z 12 FOG).

The law requires "scientific institutions" to perform a range of organizational safeguards (§2d Abs 1 FOG) and in and turn permits far reaching processing of personal data. For example, the law explicitly allows processing and storage of data on political, religious and health background including genetic data (§ 2f Abs 1 Z 6 FOG), excepts data controllers from their responsibilities Art 15-18 and 20-21 GDPR if that is likely to seriously impair the processing purposes (§ 2f Abs 6 FOG) and even allows publication of personal data if does not contain name, address or photo of the data subject (§ 2d Abs 2 Z 1 lit c lit cc FOG).

In summary, Austria implementation in the FOG appears to be on the verge of what can be considered appropriate safeguards for the rights and freedoms of the data subject required by Art 89 GDPR. For example, Art 89 does not permit exceptions from Art 17 GDPR ("Right to be forgotten") for research purposes whereas the Austrian FOG explicitly allows such exceptions.

(x) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

For research purposes all personal data including sensitive data may be processed if the processing is performed with pseudonymous data or publication is done without name, address or photo of the data subject (§ 2d Abs 2 Z 1 lit c lit cc FOG).

In the event of a natural disaster, personal data of potentially affected data subjects may be transmitted to their relatives upon request. Sensitive data may only be transmitted if the relatives if they provide evidence confirming their identity and the transmission is required for the rights of the relative or the person affected by the natural disaster (§ 10 Abs 4 DSG).

The law also contains special provisions regarding image acquisition for personal purposes. Among other requirements, image acquisition is not permitted if the captured images are analysed with sensitive data as selection criterion (§ 12 Abs 4 Z 4 DSG).

(xi) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

According to our knowledge, there are no national Codes of Conducts established specifically for the ethics of data processing in research. However, there exist a number of bodies for ethics in research and ethics in general. The "Datenschutzrat"[42] advises the federal and local governments on matters of legal politics in data protection and is located at the Federal Ministry of Constitutional Affairs, Reforms Deregulation and Justice. It issued a very critical statement of the national implementation of the research exceptions found in Art 89 GDPR[43]. Many scientific institutions have commissions for ethics, i.e. the "Kommission für Wissenschaftsethik" at the Austrian Academy of Science[44].

42 https://www.justiz.gv.at/web2013/home/verfassungsdienst/datenschutzrat~2c94848b60c168850160d54cf36f295e.de.html (german)

43 https://www.justiz.gv.at/web2013/file/2c94848a60c15838016198daa7442ac0.de.0/1_stellungnahme_des_datenschutzrates_.pdf (german)

44 https://www.oeaw.ac.at/en/members-commissions/commissions/kommission-fuer-wissenschaftsethik/ (german)

(xii) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

There is not specific definition of "statistical purposes" in the Austrian DSG. Nevertheless, processing of all personal data is permissible if no personalized results are sought and the data is publicly available, has been obtained by the data controller for other purposes or is pseudonymous for the data controller (§ 7 Abs 1 DSG). If these requirements cannot be met, the data may also be processed in accordance with special legal provisions (i.e. the FOG) or with authorization of the Austrian data protection agency (§ 7 Abs 2 DSG).

(xiii) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

Yes, such regulation resides mainly in the FOG. For details see answer to question (v) of this part

1.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

The wording in § 1 DSG may be interpreted to imply that the "personal" data of legal persons also enjoys protection under this law. This is a known issue and attempts to address this situation in the past have failed due to the political situation in the national assembly.

(ii) Are there any special requirements regarding informed consent at the national level?

Older provisions tend to use the wording "Zustimmung" (approval) instead of the term "Einwilligung" (consent) used in the GDPR. If both terms can be regarded as equivalent and therefore profit of the clarifications what constitutes an "informed" consent in the GDPR is subject to debate. A provision, which states that an older approval remains valid if it fulfils to the requirements of the GDPR, may suggest that such an equivalence was intended by lawmakers (§ 69 Abs 9 DSG).

(iii) Are there any special requirements regarding data processing at the national level?

Exceptions from the fundamental rights of data protection in § 1 DSG for national authorities may only be made by laws adhering to Art 8 Abs 2 EMRK and have to contain legal protections for the person concerned (§ 1 Abs 2 DSG). This does not apply to data processing with the approval of the person concerned or is necessary for their vital interests.

(iv) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

Within the domain of national security and cybersecurity, the data subject's rights to access and correction are limited. Biometric identification ("Erkennungsdienstliche Daten") data like fingerprints or DNA profiles may only be deleted on the subject's request if legal reason for their elicitation is the data subjects' consent (§ 74 SPG).

Otherwise the data can only be deleted ex officio. The data subject is also barred from access to their biometric identification data (§79 Abs 2 SPG).

When processing personal data for research activities, the Austrian FOG also allows to restrict the data subject's rights codified in Art 15-18 and 20-21 GDPR if exercising these rights may seriously impair the processing purposes (§ 2f Abs 6 FOG).

1.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

In a disaster situation, the data subject's personal data (including special categories), in particular their likely location, may be given to close relatives like parents or kids (§ 10 DSG). For the use of biometric data by police forces see answers to previous questions.

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

The DSG allows the consent of minors for services of the information society at the age of 14 (§ 4 Abs 4 DSG). Otherwise the DSG doesn't contain special provisions for minors.

(iii) Are there other vulnerable individuals identified in your national legislation?

The Austrian DSG does not contain special provisions for other potentially vulnerable groups.

1.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

In Austria, fundamental rights of a person cease to exist together with their bearer. The personal data of deceased individuals therefore loses the direct protection of the Austrian DSG. However, the privacy rights of living friends or relatives of the deceased still have to be respected. Regulation concerning professional secrecy of state officials, doctors or lawyers stay in force independently but have a different intrinsic purpose than personal data protection laws.[45]

1.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

Within the domain of security and cybersecurity, the SPG requires and appointment of a commissioner for legal protection. Security forces like the police have to inform the commissioner when the want to use investigative measures like audio or video recordings (§ 91c Abs 1 SPG). The commissioner may inform data subjects if he beliefs their rights to be violated by the security forces. He submits a yearly report on his findings, which the minister for interior has to make available for the relevant parliamentary

[45] http://web.archive.org/web/20180407073344/http://archiv.dsb.gv.at/site/6238/default.aspx

subcommittee on request (§ 91d Abs 4 SPG). In addition, the national government has to submit a yearly report concerning national security to parliament.

The state can be held liable if security forces failure to act caused damages to private property (§ 92 Z 1 SPG).

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

Yes, the national DSB issued a regulation containing criteria when a privacy impact assessment has to be carried out in any case.[46] For example, this includes classification or profiling of natural persons based on their locations and monitoring of public space using video or audio recordings by security forces. There also exists a regulation specifying which data processing activities do not require a privacy impact assessment, this includes scientific research and statistical purposes.[47]

For data processing in research, the scientific institution has to appoint a data protection officer if data from public registers like the database of medical records is desired (§ 2d Abs 1 Z 5 lit c FOG). If no special categories of personal data (Art 9 GDPR) are processed, data controllers are explicitly not required to perform a data protection impact assessment (§ 2k Abs 4 FOG).

1.2 Commercialization of data

1.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Konsumentenschutzgesetz (KSchG)	https://anon.to/Q6g7GG	Hard law	Consumer protection law which also contains regulations when Stipulations in the Terms of Service are inadmissible

Main regulatory tools addressing data commercialization in Austria.

1.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

[46] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010375
[47] https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.pdfsig

To our knowledge, no regulations specific for the contractual exchange of personal data as a payment for services exist. Based on national regulation, the arguments for illegality are sparse. The only reason coming to mind would be because of "unclear or incomprehensible" language in a contract between a consumer and a company (§ 6 Abs 3 KSchG). This would depend on the contract wording and cannot be determined without a concrete case.

(ii) Do you know if these practices are routinely performed?

Stipulations about the processing of personal data are routinely contained in the terms of service of companies. However, these terms of service are subject to Austrian consumer protection law and individual stipulations may be struck down on this basis (see answer to question above). These protections still apply if foreign companies offer goods or services to Austrian consumers as most of the Austrian consumer protection law is mandatory law (§ 2 Abs 2 KSchG).

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

No general regulation for all kinds of data exists. Special regulations exist for artistic works data protected by copyright, for details see the answer to the next question.

(iv) Do you have any particular national regulation on the secondary use of data?

Yes, for statistical and research purposes far reaching exceptions from the principle of purpose limitation exist. For details see the previous answer.

(v) Do you have any specific protection for metadata or non-personal data in your country?

No.

1.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

To my knowledge, data by itself is not classified in any legal category. Depending on the connection to a natural or legal person, it may fall under different legal regimes. For example, data constituting creative works by authors is protected by copyright and data pertaining to business secrets of companies are protected under the act against unfair competition. There is no overarching concept of what legal status data shall have by its own right.

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

Data which constitutes a work of art is protected under the Austrian "Urheberrechtsgesetz" (copyright law). The creator is entitled to a compensation when it is to be expected that his public available work will be copied on storage media for private purposes ("Speichermedienvergütung"). Regarding the amount of compensation, the law defines a range of criterions to take into account, including the loss of income to private copies and the advantages to the copiers (§ 43b Abs 4 UrhG). In a sense this can be regarded as a framework to determine the value of data in very specific circumstances.

1.3 Security and cybersecurity

1.3.1 General Regulatory Framework

Regulation	Link	Type of regulation (hard law, soft law…)	Brief description and scope
Netz- und Informationssystemsicherheitsgesetz	https://anon.to/LUPOvN	Hard law	Mainly contains special regulations for provides of critical infrastructure
Datenschutzgesetz (DSG)	https://anon.to/ggRI5X	Hard law	Chapter 3 contains regulations for the purposes of public security

Main regulatory tools addressing security and cybersecurity in Austria

1.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

For police forces and other bodies of national security are required to implement appropriate technical and organizational measures when processing personal data (§ 27 Abs 1 Z 6 DSG). The law sets forth a number of goals for this purpose, essentially reiterating the goals of Art 29 Abs 2 Police Directive (§ 54 Abs 2 DSG).

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The NIS directive has been implemented in Austria by BGBl I Nr. 111/2018. This resulted in a new "Netz- und Informationssystemsicherheitsgesetz" and changes to the "Telekommunikationsgesetz 2003".

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

In Chapter 2 Part 2 and 3, the Austrian DSG mainly reiterates key elements of the GDPR like the rights of the data subjects and duties of data controller and processor.

1.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

In case of a substantial number of affected users within essential branches like energy, traffic, or public health (§ 2 NISG), the data breach has to be reported to sector specific computer emergency response team (§ 19 Abs 1 NISG).

The national regulations regarding data breach notification in the DSG refer to their counterparts in the GDPR (§ 55f DSG).

1.3.4 Supervision of cybersecurity

(iv) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

To my knowledge no such body exists in Austria. Substantially cybersecurity incidences within essential branches have to be reported to the responsible CERT, but the organization has no authority issue administrative fines for non-compliance.

(v) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or something similar established? If yes, what are the competences and responsibilities?

To our knowledge no such body exists in Austria.

(vi) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

If the damages result from violations of the GDPR or the fundamental right to privacy of personal data (§ 1 DSG), they may be compensated according to the provisions of civil tort law (§ 29 Abs 1 DSG). The claim may be lodged at the competent civil court either at the claimants or the defendants' domicile (§ 29 Abs 2 DSG).

The Austrian procedural law does not contain the concept of a class action lawsuit. In cybersecurity cases, the damages caused to a single individual may be too small to warrant bearing the risk of an expensive tort lawsuit. However, the overall damage caused may be substantial due to the number of individuals affected by the cybersecurity breach. It may therefore be desirable to revise procedural law to offer remedies for these kinds of situations, i.e. by introducing class action lawsuits for such cases.

1.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

There is a specialized statuary crime called "data processing with the intent to profit or malice". Who purposefully breaches the data fundamental right to data protection (§ 1 Abs 1 DSG) with the intent to profit or malice faces imprisonment of up to 1 year or a fine of up to 720 daily rates (§ 63 DSG).

However, this only applies if the culprit doesn't face a harsher penalty by other statuary laws. "Fraudulent abuse of data processing", where one manipulates the result of data processing operations with the intent to profit, may lead to an imprisonment between 1 and 10 years, if the resulting damage exceeds 300 000€ (§ 148a StGB).

According to national law, no fines due to data protection violations may be imposed against public authorities and public corporations (§ 30 Abs 5 DSG). Whether this regulation meets the requirements of effective and dissuasive fines set forth by Art 83 Abs 1 GDPR and Art 57 RL (EU) 2016/680 remains to be seen.

(ii) Are there administrative fines related to data protection issues?

Yes, for data protection issues not covered by Art 83 DSGVO (i.e. purposefully gaining unlawful access to a data processing facility) may result in an administrative fine of up to 50 000€ (§ 62 Abs 1 DSG). In addition, equipment like storage media or cameras used for the breach can be confiscated and ownership may be transferred to the state (§ 62 Abs 4 DSG).

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

Both, "data processing with the intent to profit or malice" and "fraudulent abuse of data processing" constitute an official offence.

1.5 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

Yes, depending on the field of research specialized committees exist which also assess data protection issues in of (proposed) research projects. Within the field of gene analysis and gene therapy, the "Gentechnikkommision" (committee on gene technology) exists, which is consulted when a somatic gene therapy is performed[48][49], includes an expert on data protection.[50]

For nation research funding agencies, the situation often depends on the concrete call. Some calls require applicants to submit documents relevant for data protection, i.e. a data management plan.

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these

[48] § 75 (3) of the Austrian "Gentechnikgesetz" (GTG), StF BGBl 510/1994

[49] § 88 (1) GTG

[50]

instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

Mostly through submitting documents at proposal stage. Submitting a data management plan (DMP) is often required.

For certain documents, online tools are recommended, i.e. the Data management tool DMP online for creating data management plans. The agencies provide DMP templates[51] or link to online tools for data management.

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

No specific national legislation for dual-use of ICT technology has been found.

2 Belgium

Gianclaudio Malgieri, Andrés Chomczyk (BUV)

2.1 Informed consent

2.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law…)	Brief description and scope
Loi du 3 décembre 2017 portant création de l'Autorité de protection des données	https://bit.ly/2SleXOw	Hard law	This organic law regulates the structure and composition of the Belgian Data Protection Authority
Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (the	https://bit.ly/31vnYIH	Hard law	Implementation of GDPR in Belgium

[51] https://www.fwf.ac.at/de/forschungsfoerderung/open-access-policy/forschungsdatenmanagement/, accessed 3.6.2020