Translation from German

**Introduction to Data Use Agreements**

Nouns equally refer to all genders; male, female and other forms have been omitted for reasons of convenience only.

1. **Background information on the need for data use agreements**
   1. "Data is the new oil" is the mantra on the economic background of big data, machine learning and the technology hype surrounding data science. It is beyond doubt that many (new) business models of our information society would not be feasible without data processing as a matter of principle. Often data is also used to optimise existing models. Moreover, many of those models have become possible only due to the development and enhancement of the internet.
   2. Since automated data processing is advancing into almost all areas of our working and private lives, and more and more equipment for faster processing and exchange of data with increasingly large memory capacities is used, the volume of processed data is growing at an enormous speed. The research community proclaims: "No data, no research."
   3. These facts and (due to technology leaps - keywords: "artificial intelligence" or "quantum computers" - quite new) opportunities lead to more and more endeavours to monetise data, on the one hand, and to (potential) misuse in connection with data, on the other. For quite some time now (EU) legislators have therefore been charged with the task of reviewing current legislation as to whether the laws measure up to these new social challenges. Legislators have seen need for action in many areas and have adopted numerous standards and initiated numerous bills. Nonetheless, and in part precisely because of the new legal situation, there are legal uncertainties in connection with the use of data.
   4. Against the backdrop of
2. the necessity of data processing for business models and/or
3. the endeavours to monetise data

more and more agreements are concluded in connection with data use. The present introduction and the IPAG model agreements are intended to provide guidance on the drafting of appropriate data use agreements. Even though all texts and explanations refer to the legal situation in Austria, the IPAG model agreements' aim is to be usable as independently as possible of the underlying legal regime, so that they can be used for international projects as well. However, specifically in the case of data such endeavours soon reach their limits, as the legal nature of data is quite manifold and the relevant legal frameworks are neither harmonised nor standardised, not even in the EU. Moreover, no relevant case law is available.

* 1. Based on the assumption that it is not "data as such" that is the subject matter of data use agreements but "embodiments of data", the term "data" as used hereinafter means "embodiments of data".

1. **Introduction to the legal nature of data and data use agreements**
   1. The following chart illustrates the major features of the legal nature of data (for details see point 3 In-depth knowledge), with these definitions also being relevant to the different regulating dimensions of data use agreements and therefore to be mapped appropriately:

**Intellectual property rights**

**(IPR)**

* 1. For data use agreements the parties must therefore clarify the following issues as early as in the planning phase, among others:
  2. Insofar as personal data is the subject matter of a data use agreement, the roles of the contracting parties under data protection law, i.e. (separate or joint) controller and/or processor and/or data subject, must also be taken into consideration from the start because different rights and obligations are associated with the roles.

**‘Data subject’**  
Person whose personal data is processed

**So-called “Controller”**  
the one who determines alone or with others the purposes of and means for the processing of personal data

**Processor**processes personal data of a data subject exclusively on behalf of the controller.

The data subject is the person whose personal data is processed. Data subjects are the primary subjects protected by data protection law (i.e., in particular, the GDPR and the Austrian Data Protection Act [*Datenschutzgesetz/DSG*]) and may exercise their rights as a data subject vis-à-vis the controller (see immediately below), including, without limitation, the right of access to information and, where applicable, the right to rectification, erasure ("right to be forgotten"), data portability and/or objection.

The so-called "controller" is the main addressee of the obligations imposed by data protection law. The controller is the one who determines the purposes of and means for the processing of personal data. He must ensure the "substantive and formal lawfulness" of the processing of personal data. In doing so, he must observe the principle that the processing of personal data is prohibited unless there is a legal ground permitting the same ("substantive lawfulness"). The controller must therefore be able to rely on legal grounds for the processing of personal data, in particular on a statutory duty and/or authorisation to process data, the necessity to perform a contract entered into with the data subject, legitimate interests in processing and/or the data subject's consent. Apart from legal grounds, also statutory requirements for substantive lawfulness must be met, including, without limitation, the requirements of purpose limitation, data minimisation, accuracy, storage period limitation, data security and accountability. "Formal lawfulness" particularly concerns proper data protection information, records of processing activities, and the conclusion of mandatory agreements under data protection law (data processor agreement or agreement between joint controllers) as well as ensuring the lawfulness of any international data transfer beyond the borders of the EEA.

The processor and subprocessors, if any, are those who process personal data of a data subject exclusively on behalf of the controller. The primary duty of the processor under data protection law is to warrant data security in terms of "technical and organisational (protective) measures - TOMs". Processors also have reduced duties regarding "formal lawfulness", i.e. merely basic records of processing activities and conclusion of data processor agreements that are mandatory under data protection law.

For more information on data protection law please see section 7 below on "Clinical studies". For "Data protection law and research" please see section 8 below.

* 1. The parties involved should therefore go over the following "checklist" for data use agreements as early as possible to be able to use appropriate model agreements and to draft and negotiate appropriate regulations. In this context it has to be borne in mind, however, that some issues are excluded from party autonomy, in particular:
* Once personal data is processed at any stage of the project, the mandatory requirements of data protection law must be observed. Insofar as "sensitive personal data", in particular personal health data, is processed, the even stricter regime of processing special categories of personal data applies.
* The laws on intellectual property, in particular copyright law, provide for mandatory regulations, which cannot be modified by agreement or can be modified only under special circumstances, including, without limitation, the areas of moral rights of authors, (advance) waiver of certain rights under the (Austrian) Copyright Act [*Urheberrechtsgesetz*], etc.

1. **In-depth knowledge**
   1. Despite the endeavour of designing the IPAG model agreements on data use so that they can be used in any jurisdiction, one must understand the delineation of the legal nature of data in order to fully understand the regulatory requirements in data use agreements. And, as so often in a legal context, this means: "It depends." The following is intended to give an introduction to "that on which it depends", namely the different legal dimensions of data:
2. **In-depth knowledge: property law and "data ownership"**
   1. A distinction has to be made between
3. data, i.e. information as such (oral or stored temporarily in the main memory) and
4. "data embodiments", i.e. physical data (on paper) or data stored (on a physical data storage medium).

Re (i): In the case of data as such the regulations of property law in Austria, and even more so in other jurisdictions, reach their limits in terms of legislation and legal practice, so that "data ownership" and the statutory provisions regulating the same surely do not apply. Nonetheless, despite the regulations of property law, which are mandatory as a matter of principle and thus not subject to party autonomy, the authors assume that the parties may agree on regulations having an "effect similar to data ownership". In cases of doubt, however, such contractual regulations would be ineffective vis-à-vis third parties who are no parties who are not involved in the contract, i.e. who are no parties to the contract, and that is specifically why statutory "data ownership" would be required. Only if data ownership were to be established, would an absolute right be secured that would also be effective vis-à-vis all third parties, so that the data owner would be able to rely on the statutory provisions protecting ownership or title, including but not limited to civil-law actions for trespass or ownership-based actions for cease and desist orders, etc. Even though these instruments may be emulated in a contract, they will then exclusively apply among the parties to the contract.

Re (ii): Data embodiments, on the other hand, qualify as "(physical) property" for the purposes of the (Austrian) laws. In order to qualify as physical property, objectively ascertainable existence and controllability are decisive, with the indirect ability to do so, i.e. by means of devices, being sufficient. In this way the statutory provisions of both property law and the law of obligations could be directly applied to data embodiments, i.e. "genuine ownership of data embodiments" or "data (embodiment) ownership". Then it would actually be possible to acquire, transfer and also to lose ownership of data embodiments under the general rules of property law. Statutory protection of possession and ownership would therefore also apply to data embodiments.

* 1. Assuming that ownership of data embodiments is possible, the question arises of how ownership of newly created data embodiments is established apart from derived acquisition by transfer of title from the previous owner. In this context the following scenarios can be distinguished:

1. acquisition of title by creation: the creator of a data embodiment is its owner;
2. acquisition of title by deriving benefits from data: the usufructuary (usually the owner) of the original data embodiment is entitled to data embodiments that are automatically generated by other data embodiments;
3. special case regarding (b) - by duplication: since the content of the copy is exclusively that of the original, ownership of the copy is to be attributed to the usufructuary of the original.
   1. The newly established ownership of the data embodiments can then be used in accordance with the general regulations of property law and the law of obligations.
   2. In principle, the provisions of intellectual property law and data protection law described below do not affect the classification of data embodiments in terms of title. Rather, they "only" regulate additional, even though not fully decoupled (the authors therefore speak of the "Janus-faced character" of), legal dimensions of data (embodiments):
4. **In-depth knowledge: "The Janus-faced character of data (embodiments) under IP law"**
   1. Against the backdrop of the tension between intellectual property law (in particular copyright law and also trade mark and patent law and the like) and property law or the law of obligations (in particular warranty law) regarding computer programs, which has been controversial for long but clarified by court decisions as to wide areas now, the authors assume that the "legal nature of data (embodiments) is Janus-faced"; in other words: data (embodiments) may be subject to regulation in both areas of law and if this is the case, both regimes must be observed, and conflicting results, if any, have to be resolved by mutually influencing the interpretation of the statutory regulations. Since most of the relevant statutory provisions are not mandatory, the parties can minimise such conflicts by stipulating unambiguous contractual provisions reflecting their regulating will as clearly as possible (to the extent permitted by law). However, in cases of doubt such regulations have no effect on third parties who are no parties to the agreement.
   2. Similar to the distinction between non-physical and physical property as mentioned above with regard to "data ownership", a (certain) embodiment of proprietary items is also required in connection with intellectual property rights. In cases of doubt mere ideas, i.e. mere thoughts or pieces of information, are not protected or capable of being protected by intellectual property rights. In this respect certain parallels can be seen in the "Janus-faced character" with a distinction between
5. data as such and
6. data embodiments.

In this context it should be borne in mind that intellectual property law constitutes a special law the provisions of which apply to data embodiments only to a small extent.

* 1. In order to be protected by copyright, data embodiments would have to be a "proprietary intellectual creation" as defined by the Copyright Act. For database protection, which is also regulated in the Copyright Act, "capital expenditure which is substantial as to type or volume" would have to be incurred in connection with the procurement, verification or presentation of the data embodied in the database; a possible criterion for being capable of legal protection which is definitely not always met.
  2. For protection under trade mark or patent law the data embodiments would have to be registered in the relevant registers with statutory criteria applying in this regard, which may be reviewed *ex officio* by the patent or trade mark offices. Therefore, it cannot be excluded that data embodiments may also be the subject of such intellectual property rights, but this can only be dealt with on a very specific case-by-case basis.
  3. Where it is clear or cannot be excluded that there are (or may be) intellectual property rights in such data embodiments, the data use agreements should address this dimension as well.

1. **In-depth knowledge: "The Janus-faced character of data (embodiments)"**
   1. In view of the data protection law dimension data (embodiments) may also be "Janus-faced". Also here both regimes must be observed and conflicting results, if any, have to be resolved by mutual influence on the interpretation of the regulations. However, since the provisions of data protection law (as a "public law") are mostly withdrawn from party autonomy, the contracting parties' options to resolve conflicts by means of contractual regulations are limited. In other words: due to their mandatory nature the regulations of data protection law prevail over the regulations regarding ownership and/or intellectual property in the case of conflicting results.
   2. With respect to the potential data protection law dimension of data use agreements three scenarios must be strictly distinguished:
2. data protection law does not apply to "anonymous data", which means that the data protection law dimension may be disregarded;
3. data protection law is applicable to "personal data", including "pseudonymised data";
4. special requirements of data protection law apply to "sensitive data":
   1. Re (i) - anonymous data: this type of data is not defined by data protection law. It is distinguished by reverse conclusion from the legal definition of "personal data", in other words: data other than personal data is anonymous data. Consequently, the principles of data protection should not apply to anonymous information, i.e. information which does not relate to an identified or identifiable natural person, or personal data which has been anonymised in such a way that the data subject cannot or can no longer be identified (Recital 26 of the GDPR). With respect to the dimension of "identifiability" there is a "flexible system" because all means which, according to general discretion, are likely to be used to directly or indirectly identify a person must be taken into account. In assessing whether means are, according to general discretion, likely to be used to identify a natural person, all objective factors must be taken into consideration, including, without limitation, the costs of and time required for identification. For this purpose the technology available at the time of processing and technological developments must be considered. An anonymisation procedure will reasonably prevent re-identification (at least in a data protection environment) if it provides a solution for three risks, namely:

(a) singling out,

(b) linkability and

(c) inference.

In this context the purpose of an *ex-ante* evaluation would be to determine, according to general discretion, the degree of probability of establishing a link to a person in the specific data sets in an *ex-post* evaluation. For this purpose, the following evaluation dimensions should be used in the sense of a "flexible evaluation system":

(aa) means likely to be used according to general discretion to establish a link to a person and in this connection:

1. the nature, volume, context and purpose of processing;
2. probability of occurrence and severity of the risk to the rights and freedoms of the data subjects;
3. costs of identification and
4. the time required,
5. with the technology available at the time of processing and technological developments having to be considered.

If (bb) one arrives at the conclusion that re-establishing a link to a person is not to be expected except with disproportionate effort, data is considered to be anonymous.

If the subject matter of a data use agreement is solely anonymous data, apart from the warranty of all parties to the effect that they will refrain from establishing links to persons in any case, the data protection law dimension may be disregarded.

* 1. Re (ii) - personal data: the definition of "personal data" by data protection law is a very broad one and means "all information relating to an identified or identifiable natural person (hereinafter "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4 No. 1 GDPR).

The classification as "personal data" is of high practical relevance because data protection law is based on the "principle of prohibition subject to the proviso of consent"; in other words: processing of personal data is prohibited as a matter of principle, unless the processor can rely on a legal ground permitting processing ("substantive lawfulness") and complies with the framework conditions of data protection legislation, including but not limited to data security, rights of data subjects, records of processing activities, data protection agreements and the like ("formal lawfulness").

Substantive and formal lawfulness of the processing of personal data is derived from the principles (Article 5 GDPR - referred to as "data protection law requirements" by the authors); according to them lawful processing requires that personal data

(a) is processed lawfully, fairly and in a transparent manner in relation to the data subject (requirements of "lawfulness, fairness and transparency").

As to the requirement of lawfulness see the more detailed information on legal grounds (Article 6 GDPR and for "sensitive data" Article 9 GDPR).

(b) is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (requirement of "purpose limitation").

However, interpretation of the requirement of purpose limitation should not be overly strict (cf. also Article 6(4) GDPR). For example, setting up a test database parallel to another database may still be covered by the principles of purpose limitation and legitimate interests (ECJ C-77/21) so that there is still some "leeway" regarding data use agreements in this respect.

(c) is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (requirement of "data minimisation").

(d) is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (requirement of "accuracy").

(e) is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (requirement of "storage limitation").

(f) is processed in a manner that ensures appropriate security of the personal data (requirements of "integrity and confidentiality").

with the controller having to be able to demonstrate compliance with (a) to (f) ("accountability").

As to the requirement of lawfulness: processing of personal data is exclusively permitted on the basis of one of the following legal grounds, some of which are specified in more detail in the regulation (for details see Article 6 GDPR): (aa) consent to processing for one or more specific purposes (for the requirements of lawful consent cf. also Article 7 GDPR); (bb) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (cc) processing is necessary for compliance with a legal obligation; (dd) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (ee) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (ff) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject (this criterion does not apply to processing carried out by public authorities in the performance of their tasks).

* 1. Re (iii) - "sensitive data": (even) stricter regulations of data protection law apply to this category of personal data, which requires a high level of protection. Here it has to be kept in mind that an exhaustive list of "sensitive data" has been defined, namely personal data revealing (a) racial or ethnic origin, (b) political opinions, (c) religious or philosophical beliefs, or (d) trade union membership, and (e) genetic data, biometric data for the purpose of uniquely identifying a natural person, (f) data concerning health or (g) data concerning a natural person’s sex life or sexual orientation (Article 9 GDPR). Re (f) - health data is defined as personal data relating to the physical or mental health of natural persons, including the provision of health services, which reveals information about their state of health (Article 4 No. 15 GDPR).

For data use agreements the relatively broad meaning of "sensitive data" has to be taken into account as well, because also "indirectly sensitive data" fall under the strict regime (ECJ C-184/20).

Processing of "sensitive data" is exclusively permitted on the basis of the following legal grounds, some of which are specified in more detail in the regulation (for details see Article 9 GDPR):

(aa) explicit consent;

(bb) processing is necessary under labour and employment law;

(cc) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(dd) processing is carried out by an organisation with a political, philosophical, religious or trade union aim on the basis of appropriate safeguards;

(ee) processing relates to personal data which is manifestly made public by the data subject;

(ff) enforcement of legal claims;

(gg) statutory authority;

(hh) processing is necessary for the purposes of preventive medicine by professionals who are subject to professional secrecy;

(ii) processing is necessary in the area of public health and/or

(jj) processing is necessary for (statutory) archiving purposes, scientific or historical research purposes or statistical purposes.

Apart from the above substantive-law requirements, increased data security measures may have to be implemented for data use agreements for lawful processing of "sensitive data" (cf. Article 32 GDPR).

Even if they constitute no "sensitive data" in the formal sense, the processing of personal data relating to criminal convictions and offences (which terms are to be understood very broadly) is subject to special restrictions (Article 10 GDPR). As a matter of principle, processing may be carried out only under the control of official authority or when the processing is authorised by law (cf. in this connection Section 4(3) *DSG*). Any comprehensive register of criminal convictions may be kept only under the control of official authority.

* 1. The central addressee of the statutory provisions of data protection law is the "controller", i.e. the one who determines the purposes of and means for processing (Article 4 No. 7 GDPR). The controller is responsible for ensuring the lawfulness of all data processing activities both as to "substance" (lawfulness in the narrower sense) and "form" (compliance with the "formal requirements" under data protection law, such as safeguarding the rights of data subjects, including, without limitation, data protection information, data security throughout the processing chain, full records of processing activities and the like).
  2. This role has to be distinguished from that of the "processor", i.e. the one who processes personal data on behalf of the controller (Article 4 No. 8 GDPR). In principle, the processor has no "substantive duties" (he is not normally responsible for ensuring lawfulness in the narrower sense) and is only subject to reduced "formal duties" (data security in his sphere of control, basic records of processing activities and the like).
  3. The subject of protection of data protection law is the data subject, i.e. the one whose personal data is processed (cf. Article 4 No. 1 GDPR).

1. **In-depth knowledge: Data and clinical studies**
   1. So-called "clinical studies" on pharmaceuticals (see the definition in Section 2a of the Austrian Pharmaceuticals Act [*Arzneimittelgesetz/AMG*]) necessarily lead to the generation and later to processing of personal health data of the test persons or patients ("study participants"). Section 41 *AMG* provides that study participants, or if they are not capable of making a decision, their legal representatives, must be expressly informed, namely in writing, about the purpose and scope of collecting and processing personal data (which may not only be that of the study participant) and give their consent to data processing. This means that the requirements for consent to clinical studies are stricter than those under general data protection provisions (in particular Articles 7 and 9 GDPR). Section 41(3) *AMG* also regulates processing in the special case that a study participant dies or that the study ends after the study participant was informed but before he gave his consent.
   2. On the other hand, such *AMG* consent constitutes a broader legal ground than a general consent: for withdrawal of *AMG* consent by the study participant neither affects any "activities" carried out on the basis of the *AMG* consent before its withdrawal nor any processing of data that was collected on that basis (Section 41(2) *AMG*).
   3. The Pharmaceuticals Act excludes the right to erasure ("right to be forgotten" - Article 17 GDPR) and the right to data portability (Article 20 GDPR). However, this must explicitly be pointed out when obtaining consent (Section 41(2) *AMG*).
   4. As in every assessment under data protection law, it is very important also in clinical studies to correctly assign the roles of controller and processor in order to comply with the obligations arising from data protection law (also according to the *AMG*). The three main roles in clinical studies are (i) the study participants (test persons or patients as data subjects), the sponsor (mostly the pharmaceutical organisation) and the investigator (the physician carrying out the study). The *AMG* does not regulate the role of the sponsor and that of the investigator in terms of data protection law, which means that they have to be identified according to general data protection standards and may differ depending on the processing step:
   5. Accordingly, depending on the specific arrangement as to who determines the purpose and means of data processing, a case-by-case evaluation will be required as to whether and when there is separate or joint responsibility (Article 26 GDPR) or, in exceptional cases, even processing on behalf of the controller (Article 28 GDPR). Due to the direct contact, the information duty and the direct collection of the study participant's data by the investigator, he will normally be the one who (at least in this regard - cf. also Section 43(4) Nos 1 and 2 *AMG*) determines the purpose and means of data processing; the more specifically the sponsor (co-)determines such purposes and means, the more likely it is that joint responsibility applies. Subsequently, responsibilities will normally be separate as the sponsor will then pursue his own purposes and means with the (pseudonymised) data transmitted to him. Therefore, the investigator and the sponsor must define the exact circumstances of the different processing steps to assign the relevant roles under data protection law. In this connection Section 43(4) *AMG* provides (which means that agreements between the investigator and the sponsor must follow such guidance) that the investigator is responsible for (i) correct data processing, i.e. collection, recording and transmission; (ii) pseudonymising the data as early as possible, documenting such pseudonymisation, handling the documentation with utmost care and ensuring that data will be linked to a specific data subject (= study participant) exclusively in the circumstances defined in the study protocol; (iii) compliance with the (remaining) obligations according to the rights of data subjects (Articles 13, 15, 16 and 18 GDPR) and (iv) communicating to the study participant any data breaches (cf. Article 34 GDPR) and to notify the sponsor thereof.
   6. Independent of the above assignment of roles, the Pharmaceuticals Act refers to Section 2d(3) of the Austrian Research Organisation Act [*Forschungsorganisations­gesetz/FOG*] regarding any further processing of data collected and/or processed in the course of the clinical study; see below.
   7. For the sake of completeness: except for the special case of the death of a study participant the above also applies to non-interventional studies.
2. **In-depth knowledge: Data protection law and research** 
   1. In certain areas the European legal framework for data protection (GDPR), which is in principle directly applicable in some areas, provides for so-called "opening clauses", which grant legislators of the Member States margins of manoeuvre for their national legislation. Implementing Article 9(2)(j) GDPR and Article 89 GDPR, Austria enacted Section 7 *DSG* (which mainly follows the old Section 46 *DSG 2000*) and the Research Organisation Act (*FOG*). According to the Explanatory Notes of the legislator the Research Organisation Act is to prevail over the provisions of Section 7 *DSG*, which means that that Section is *de facto* inapplicable in the field of research; consequently, only *FOG* aspects will be dealt with hereinafter.
   2. The Research Organisation Act (*FOG*) provides for extensive privileges and simplifications (which may even go too far and violate European law) of the data protection framework for the processing of personal data for scientific institutions. These are defined quite broadly, namely as "natural persons, organisations and legal entities pursuing [research] purposes [...], i.e. activities in the fields of research and experimental development [...], irrespective of whether the activities are carried out (a) for non-profit purposes (Section 34 *et seq.* of the Austrian Federal Tax Code [*Bundesabgaben­ordnung/BAO*] or not or (b) in an academic, business or non-academic context".
   3. The Research Organisation Act thus provides far-reaching permissions, some prerequisites of which are worded very abstractly. Pursuant to the "legal definition" (Section 2d(2) No. 1 *FOG*) (almost) all data processing methods are permitted in the area of research on the only condition that the controller must comply with certain "data security measures": scientific institutions (see the broad definition above) are permitted to process personal data for research purposes in any case, including, without limitation, in connection with big data, personalised medicine, biomedical research, biobanks and data transfer to other scientific institutions or processors, provided that (a) sector-specific personal identifiers or other unique identifiers are used for allocation instead of the name or (b) processing is carried out in a pseudonymised form or (c) data is (aa) not published at all or (bb) published in an anonymised or pseudonymised form only or (d) processing exclusively serves the purpose of anonymisation or pseudonymisation and involves no disclosure of directly personal data to third parties.
   4. The Research Organisation Act also privileges so-called "register research". Scientific institutions (including holders of a valid certificate as per Section 2c(2) *FOG*) may ask controllers that keep registers prescribed by federal law (except for registers kept in the areas of the judiciary, lawyers and notaries within the relevant statutory areas of activities, and the register of convictions, and in the case of ELGA [electronic health record in Austria] the register kept by the ELGA ombudsperson) for access to data from such registers in electronic form which allows no identification of data subjects or business entities through their name, address or by means of a publicly accessible identification number, provided that (a) processing (aa) exclusively serves the purposes of life and social sciences and (bb) is also in the interest of the public, (b) the register is listed in a Regulation issued by the Minister of Science, (c) the costs for granting such data access are reimbursed and (e) where matching of available data is requested, the relevant sector-specific personal identifiers of the data subjects are made available when data access is requested.
   5. In addition, scientific institutions may, in particular, collect, archive and systematically record research material (Section 2b No. 6 *FOG*) for research purposes and may process all relating data necessary to warrant optimum access to data and research materials for "register" purposes (for details see Section 2f(1) and (2) *FOG*).
   6. Moreover, data and research material which was processed to serve as a basis for research activities ("raw data") may be processed as of publication of the results of such activities (i) to prove compliance with good scientific practice for at least ten years and (ii) for up to 30 years for asserting, exercising or defending of legal claims (Section 2f(3) *FOG*).
   7. Processing in connection with biological sample collections and data collections for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety in health care and of medicinal products/pharmaceuticals or medical devices, constitutes permitted processing. Controllers must in any case implement the following appropriate and specific measures: (i) fastest pseudonymisation possible where the processing purposes can still be achieved, as well as (ii) compliance with the necessary data security measures.
   8. For teaching purposes, in particular writing of seminar and exam papers, Bachelor's theses or academic or artistic works by students, all personal data may be processed if it is ensured that, apart from permitted processing, no data will be transmitted to any recipients for other purposes.
   9. For purposes of medical research and death-related analyses the federal agency Statistics Austria is authorised to transmit the date of death and the cause of death of data subjects to scientific institutions upon agreement on the specific areas of application and reasonable reimbursement of costs. With respect to such data scientific institutions and their members are subject to an obligation to maintain secrecy as defined in the Austrian Federal Statistics Act [*Bundesstatistikgesetz*] and may use such data exclusively for scientific purposes. At medical universities or universities where a medical faculty has been established the Ethics Committee (Section 30 of the Austrian Universities Act [*Universitätsgesetz/UG*]) must be consulted before such data is transmitted. At other scientific institutions an Ethics Committee as defined in Section 8c of the Austrian Hospitals and Sanatoriums Act [*Krankenanstalten- und Kuranstaltengesetz/KAKuG*], if any, or a similar ethics committee must be consulted.
   10. Furthermore, image processing for scientific purposes is privileged under Section 44 *KAKuG*. Both automated alignment of personal data obtained from images with other personal data, and analyses of personal data obtained from images on the basis of special categories of personal data (Article 9 GDPR) as a selection criterion for research purposes are permitted, provided that (i) the processing is done by the scientific institutions and (ii) no personal data is published as a consequence of processing.
   11. Unless the above privileges apply anyhow, Section 2d(3) provides that personal data may be processed in the area of research on the basis of a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him, and in this context the purpose may be indicated by stating (i) a research area or (ii) several research areas or (iii) research projects or (iv) parts of research projects ("broad consent").
   12. Pursuant to Section 2h *FOG* scientific institutions are authorised (i) to publish the name, a photo and a list of the publications of scientific staff who are in a valid working relationship with the relevant scientific institution (a) on a website of the scientific institution or (b) in publicly accessible reports of the scientific institution, unless the publication is likely to violate public safety and order, the administration of justice, comprehensive national defence, foreign relations or a legitimate private or business interest, with the option to object to publication of a photo as per (a) above at any time, or (ii) to publish the names of scientific staff who are no longer in a valid working relationship with the relevant scientific institution, and of students (a) on a website of the scientific institution or (b) in publicly accessible reports of the scientific institution, unless the publication is likely to violate public safety and order, the administration of justice, comprehensive national defence, foreign relations or a legitimate private or business interest, or (iii) to process the following data of former scientific staff or former students and to link it with other publicly accessible information, including but not limited to: (a) research focuses and (b) information on publications, or (iv) to process information on natural persons, such as (a) names, (b) personal characteristics and (c) information on the curriculum vitae of scientists and persons related to them.
   13. On the conditions of the "legal definition" (see above) knowledge transfer is permitted. Section 2i *FOG* provides for a privilege for transfer of knowledge and technology. Irrespective of any patent-law provisions, processing, and the transmission of personal data in particular, is permitted for technology transfer if (i) such processing is necessary to obtain the functionality of the technology to be transferred and (ii) it is ensured, in particular by technology engineering, that third parties will not be able to obtain actual knowledge of the data transferred. In that case the rights of data subjects (Articles 12 to 22 GDPR) and the data breach notification duties (Article 34 GDPR) will not apply.
   14. If personal data is provided voluntarily by the data subjects themselves in connection with open-science and citizen-science projects, processing of such data is permitted in the way, to the extent and for the duration explicitly communicated at the start of the project (Section 2i(4) *FOG*). Erasure is permitted only if (i) the project goals and (ii) the methodological, in particular statistical, requirements of scientific work are not compromised. If personal data of third parties is provided in connection with open-science and citizen-science projects, processing of such data in the way, to the extent and for the duration explicitly communicated at the start of the project is permitted whenever (i) the data is based on observations or measurements in public space or (ii) the data is pseudonymised. Erasure is permitted only on the above conditions.
   15. Finally, the "internationality of processing for research purposes" is privileged (Section 2j *FOG*). Transfers to (a) scientific institutions, (b) funding and grant agencies, (c) expert witnesses, (d) Austrian public agencies (Section 2b No. 8 *FOG*), and knowledge and technology transfers to EU Member States are permitted.
   16. Apart from the above-mentioned privileges regarding substantive lawfulness, the Research Organisation Act also provides for privileges regarding formal lawfulness of processing of personal data in the area of research:
3. personal data may be stored and, where necessary, processed further for those purposes for an unlimited period of time, unless the law provides for limitations in time (Section 2d(5) *FOG*).
4. The following rights of data subjects are not applicable in the field of research if they are expected to render impossible or seriously compromise the achievement of research goals: (a) the data subject's right of access to information (Article 15 GDPR), (b) the right to rectification (Article 16 GDPR), (c) the right to erasure or the right to be forgotten (Article 17 GDPR), (d) the right to restriction of processing (Article 18 GDPR), (e) the right to data portability (Article 20 GDPR) and (f) the right to object (Article 21 GDPR).
   1. However, apart from the privileges, there are also supplementary duties under the *FOG* that must be fulfilled, including, without limitation:
5. log records must be kept on automated processing of data to allow tracking of processing activities actually carried out, such as, in particular, changes, retrievals or transfers, as to whether they are permitted to the extent necessary;
6. controllers and processors who process personal data on the basis of this section, and their staff, i.e. employees and persons comparable to employees, must keep secret personal data that has been entrusted or made accessible to them, without prejudice to other statutory obligations to maintain secrecy, unless there is a legitimate reason for the transmission of personal data that has been entrusted or made accessible to them (data secrecy);
7. natural persons whose personal data is processed on the basis of the *FOG* must suffer no disadvantages from processing, with processing in accordance with the *FOG* constituting no disadvantage.
8. Controllers whose processing activities are based on the *FOG* must:
9. indicate use of that legal basis on a publicly viewable website;
10. delete names and other personal identifiers (apart from the sector-specific personal identifier "Research" (bPK-BF-FO) and encrypted sector-specific personal identifiers (vbPK)) whenever sector-specific personal identifiers are attributed to their data;
11. appoint a Data Protection Officer (cf. Article 37 GDPR) before they use registers (see above re "register research");
12. expressly define a schedule of data processing tasks among organisational units and staff;
13. make data processing subject to valid instructions from the organisational units and staff authorised to give such instructions;
14. inform each staff member about their duties under data protection law, including data security requirements;
15. regulate the right of physical access to premises where data is processed;
16. regulate access authorisation for data and programs and the protection of data storage media against viewing or use by unauthorised persons;
17. define the authorisation for operating data processing devices and protect each device against unauthorised use by taking precautionary measures on the machines or programs used;
18. document the measures taken under (d) to (i) to make monitoring and the preservation of evidence easier;
19. in their request for access to data provide the following details in the case of "register research" (see above):

(aa) the reasons why the research project can only be realised if the envisaged access to data is granted;

(bb) the natural persons who should be granted access to data;

(cc) the data sets for which access is required and the methods used for analysing the same, and

(dd) the results to be achieved by the research project;

1. in the case of "register research" ensure that only the natural persons stated in the request will be authorised to access such data;
2. in the case of "register research" delete any names transmitted after the relevant purposes have been achieved.
   1. For details on the sector-specific personal identifiers for the area of "research" (bPK-BF-FO) see Sections 2c, 2d(2) (in particular No. 2) and 2d(9) *FOG*. Personal identifiers must in no case be published (Section 2d(1) No. 6 *FOG*).
   2. The Research Organisation Act also provides for privileges regarding penalties and other legal consequences of violations of data protection law: pursuant to Section 30(5) *DSG* such consequences are generally excluded for public authorities and public agencies. By means of Section 2k(2) No. 12 *FOG* the group of privileged persons was expanded to include processors acting on behalf of public authorities or public agencies.