‘Big data analytics’ and processing of health data for scientific research purposes : The Austrian legal framework.

Research Protocol by Max Mosing and Juliane Messner for GEISTWERT Rechtsanwälte Lawyers Avvocati *(www.geistwert.at)*
in Vienna, Austria *(contact: max.mosing@geistwert.at)*

Contents

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

1. Overview of the legal framework

a. Which laws regulate the processing of health data for research purposes (the current regime, in force till 25 May 2018)

What are the relevant applicable provisions governing the processing of health data in your country? Please provide online references (also to an English version, if available), a brief description and any specific relevant information.

In Austria, the processing of personal health data (also for scientific and research purposes) is not uniformly regulated in one act/ regulation. The provisions on processing of personal health data – as far as such provisions exist under the current Austrian legal framework – are stipulated in the relevant/ material laws. However, subsidiary (and therefore generally) applicable on the processing of personal health data for scientific and research purposes is section 46 of the Austrian Federal Act concerning the Protection of Personal Data:

Federal Act concerning the Protection of Personal Data 2000 ("*Datenschutzgesetz 2000 – DSG 2000*")[1]

The DSG 2000 governs the collection and the processing of personal data in transposition of the Directive 95/46. The DSG 2000 stipulates a constitutionally guaranteed fundamental right on data protection in its section 1 (also concerning legal persons) and a special provision for data processing for scientific research and statistics in section 46 DSG 2000. However, it is worth mentioning already at this stage that in Austria – as the DSG 2000 stipulates that most provisions are not applicable on "indirect personal data" – most projects in Austria concerning the processing of health data are working the pseudonymised (health) data.

As mentioned above, the relevant/ material laws stipulate the special provisions governing the processing of personal health data in Austria:

Relevant laws in Austria in context of processing of health data, especially for research purposes:

i. The Austrian Pharmaceutical Act ("*Arzneimittelgesetz – AMG*"[2]) and the Austrian Act on Medical Devices ("*Medizinproduktegesetz – MPG*"[3]): Both contain specific provisions for the processing of personal health data, however "only" for clinical studies.

ii. The Austrian Act on Genetic Engineering ("*Gentechnikgesetz – GTG*"[4]): It stipulates the provisions on genetically modified organisms, the release and the placing of genetically modified organisms on the market and the application of gene analysis and gene therapy on humans and contains in its section 71 et

[1] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597 (in German) and bilingual version in English: until May 24, 2018: http://archiv.dsb.gv.at/DocView.axd?CobId=41936 and from May 25, 2018 on: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.

[2] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10010441 (in German).

[3] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10011003 (in German).

[4] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10010826 (in German).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

sqq and its section 106 specific conditions for the processing and further processing of health data in this context.

iii. The Austrian Federal Act on the "Austrian Health Ltd" ("*Bundesgesetz über die Gesundheit Österreich GmbH*"[5]) lays down the provisions on the national research and planning institute for the healthcare sector in Austria. It contains in its section 15 special provisions on data protection and confidentiality in these regards.

iv. The Austrian Federal Act on Patients' Charta ("*Vereinbarung zur Sicherstellung der Patientenrechte*"[6]): this Act contain provisions for the declaration of consent concerning the processing of health data for clinical trials and research purposes in its Article 20, namely:

"No one's data may be used for clinical trials and for research and teaching purposes without the explicit consent of the data subject. The consent may be revoked at any time. The use of personal data for medical research purposes requires the explicit consent of the data subject. It is particularly important to ensure that the fundamental right to privacy is respected."

v. At a (more or less) technical level, the Federal Act on Data Security Measures when using Personal Electronic Health Data 2012 ("*Gesundheitstelematikgesetz – GTelG 2012*"[7]) and the Regulation on Data Security Measures when using Personal Electronic Health Data ("G*esundheitstelematikverordnung*"[8]) deal with the security measures of the processing of personal health data. Objectives of those regulations are to foster and extend data security when using electronic health data in directed or undirected communication by setting up uniform federal minimum standards and avoiding abuse of data; to provide and broaden the information basis necessary for the steering and development of e-health in Austria; as well as to create uniform rules for undirected communication of electronic health data.

Shared electronic health/ patient records are indirectly relevant in this context because they can potentially be an important source for health-related research.

The Austrian Electronic Health Record – EHR ("*Elektronischer Gesundheitsakt – ELGA*") was established by the above mentioned Federal Act on Data Security Measures when using Personal Electronic Health Data 2012 ("*Gesundheitstelematikgesetz – GTelG 2012*"[9]). The EHR is defined as "an information system providing all authorized EHR-Healthcare Providers and EHR-Participants with health data in electronic form, without reference to location and time (undirected communication)". Therefore, the EHR is an electronic network of the health data of patients, who emerge distributed in the health service. In addition to the patients, however, access is only available to the treating physicians or healthcare providers. The introduction of ELGA meets the requirements of Article 19 of

[5] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004884 (in German).

[6] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004633 (in German).

[7] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120 (in German) and bilingual Version in English: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2012_1_111/ERV_2012_1_111.html .

[8] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008732 (in German).

[9] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120 (in German) and bilingual Version in English: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2012_1_111/ERV_2012_1_111.html .

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the Patients' Charta[10] regarding the right of patients to access their documentation of diagnostic, therapeutic and nursing care. The data made available so far via ELGA are: medical and nursing discharge letters from public hospitals, laboratory findings, radiology findings and medication data. It is planned that also patient decrees, precautionary powers and statutory medical registers are made available via ELGA. Any person with an Austrian social security number who is being treated or looked after in the Austrian health system will in principle participate in ELGA, but there is the possibility to opt-out of the participation partially or generally.

b. Revision of the current legal framework under the GDPR

How are the necessary changes to the national data protection framework introduced by the GDPR addressed in your country? What is the adopted legislative approach?

On 25 May 2018 the Austrian Federal Act amending the Act concerning the Protection of Personal Data 2000 ("*Datenschutzgesetz – DSG*") will enter into force. However, the constitutional provisions in the DSG 2000 (sections 1 to 3, 35 (2), 60 (8), and 61 (4)) are not changed and will remain in the DSG – therefore the Austrian data protection law will also cover legal persons. Background of the keeping of the constitutional provisions is that a change could only be implemented by means of a qualified two-thirds majority in the Austrian Parliament, which could not be reached because of governmental crises in Austria before the last elections. Therefore, even though the title of the new act expressly refers to the protection of data of natural persons, there remains an Austrian characteristic that the protection of data of legal persons is covered by the DSG 2000. It remains to be seen what problems will arise in this context in practice.

Nevertheless, the DSG formally removes all provisions of the DSG 2000 except the above named constitutional provisions. However, the DSG uses some of the opening clauses contained in the GDPR, also in the context of the use of data for scientific research purposes.

Furthermore, and in the context of the AEGLE project of high relevance might be the Austrian Data Protection Adaptation Act for Science and Research 2018 ("*Datenschutzanpassungsgesetz Wissenschaft und Forschung 2018*"), which however is currently only in the status of a draft/ bill.[11]

c. The national data processing authority

Can you provide a short description of the role of the data protection supervisory authority in your country in the domain of processing health data for research purposes under the current legal framework?

[10] Article 19 (1) The right of the patients to inspect the documentation of the diagnostic, therapeutic and nursing measures including any supplements, such as X-rays, is to be ensured. (2) Restrictions are only permitted insofar as they are unavoidable due to the particular circumstances of the individual case for the benefit of the patient or the patient. A representative of the patient also has an unrestricted right of inspection in such a case, unless the patient has ruled out this.

[11] https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00010/ (in German).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The National Data Protection Authority in Austria is the "*Datenschutzbehörde – DSB*" which is governed by the DSG 2000 (and in the future by the DSG).

According to section 17 DSG 2000, any use of personal data must be notified to the DSB for registration in the Data Processing Register ("*Datenverarbeitungsregister – DVR*"). There are some exceptions of the compulsory notification[12] stipulated in section 17 (2) and (3) DSG 2000. Data applications (subject to notification), which involve sensitive data, such as health data, may only be initiated after an examination and prior approval by the DSB.

In the context of the use of personal data for scientific research section 46 DSG 2000 lays down that a permit by the DSB can substitute the general requirements of (a) a specific legal provision or (b) the consent of the data subject: A permit must be granted by the DSB for the use of personal data for purposes of scientific research upon request by the Controller if (i) the consent of the data subjects is impossible to be obtained, because those data subjects cannot be reached or the effort would otherwise be unreasonable; and (ii) there is a public interest in the use of the personal data; and (iii) the professional aptitude of the applicant/ the Controller has satisfactorily been demonstrated to the DSB. However, if sensitive data are to be collected an important public interest in the research must exist. Furthermore, it must be ensured that the personal data is only processed by persons, who are subject to a statutory duty to confidentiality or are otherwise credible. In case third party's data are used, an application with the DSB for the processing of sensitive data for research purposes must be accompanied by a statement signed by the person authorized to dispose of the collection of information from which the data shall be collected or by another authorized person that he/she makes available the collection of information for the research. The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.

However, if only "indirect personal health data" (= pseudonymised health data) are processed, no notification to and no permit/ approval by the DSB is required.

Can you describe the adopted or proposed changes to this role of the national data protection authority to ensure compliance with the GDPR?

The DSG will lay down the tasks of the DSB, which will considerably be extended in comparison to the DSG 2000. However, the Austrian legislator has "only" specified tasks that are laid down in the GDPR and has not extended them.

It is worth mentioning that with the entering into force of the DSG on May 25, 2018, the duty to notify and register data applications with the DSB will vanish.

[12] Data applications not subject to notification are applications: 1. which solely contain published data or 2. whose subject is the management of registers and catalogues that are by law open to inspection by the public, even if a legitimate interest for doing so must be demonstrated or 3. which contain only indirectly personal data or 4. which are carried out by natural persons for activities that are entirely personal or concern just the person's family life (Art 45) or 5. which are carried out for journalistic purposes according to Art 48 or 6. correspond to a standard application. The Federal Chancellor can lay down in an ordinance that some types of data applications and transmissions are standard applications, if they are carried out by many controllers in similar fashion and if a risk to the data subjects' interest in secrecy deserving protection is unlikely considering the purpose of the use and the processed categories of data. The ordinance shall list for every Standard Application the authorised categories of data, the categories of data subjects and recipients as well as the maximum period of time during which the data may be stored.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

2. Transposition of Article 8.4 of Directive 95/46

Did your national legislator insert any additional exemptions for the processing of health data for research purposes? How is it/are they formulated? Please explain. Are there additional exemptions issued by the DPA?

Art. 8.4 of Directive 95/46 reads as following: "4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority."

a. Transposition of Article 8.4 of Directive 95/46

In Austria, data concerning health are qualified as a special category of personal data (so called "sensitive data") and as such its processing is prohibited under the DSG 2000. However, the prohibition of processing of sensitive data does not apply, if the interests in secrecy deserving protection of the data subjects are not infringed and the Austrian legislator extended the list of exemptions of Article 8.4 of Directive 95/46 by a few points, amongst others the use of (sensitive) data for scientific research or statistics pursuant in section 46 DSG 2000 or the use of "indirect personal data".

b. The regime applying to the processing of personal data for health research purposes

Is there a specific regime applying to data processing for research in the field of health purposes?

As mentioned above, section 46 DSG 2000 shall only apply if there are no specific provisions regarding the use of personal data in the field of scientific research and statistics in relevant/ material law.

In fact, section 46 DSG 2000 distinguishes between three categories of use of personal data for the purpose of scientific research, namely

i. for the purpose of specific scientific research projects whose goal is not to obtain results in a form relating to specific data subjects,

ii. research projects that are not specific, but whose goal is not to obtain results in a form relating to specific data subjects, and

iii. those projects whose goal is to obtain results in a form relating to specific data subjects.

Concerning i. specific projects whose goal is not to obtain results in a form relating to specific data subjects the Controller shall have the right to use all data that (i) are publicly accessible or (ii) the Controller has lawfully collected

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

for other research projects or other purposes or (iii) are only indirect personal data[13] (= pseudonymised data) for the Controller. Other data than those named in (i) to (iii) shall only be used under the below named conditions:

Concerning i. specific project whose goal is not to obtain results in a form relating to specific data subjects, but where data shall be used not falling under the conditions (i) to (iii) named above and/ or ii. projects that are not specific or iii. whose goal is to obtain results in a form relating to specific data subjects any personal data shall only be used (a) based on specific legal provisions or (b) with the (based on Austrian case law[14]: informed and specific) consent of the data subject or (c) with a permit of the DSB.

Therefore, a permit by the DSB can substitute the general requirements of (a) a specific legal provision or (b) the consent of the data subject. A permit must be granted by the DSB for the use of personal data for purposes of scientific research upon request by the Controller if (aa) the consent of the data subjects is impossible to be obtained, because those data subjects cannot be reached or the effort would otherwise be unreasonable; and (bb) there is a public interest in the use of the personal data; and (cc) the professional aptitude of the applicant/ the Controller has satisfactorily been demonstrated to the DSB. However, if sensitive data are to be collected an important public interest in the research must exist. Furthermore, it must be ensured that the personal data is only processed by persons, who are subject to a statutory duty to confidentiality or are otherwise credible. In case third party's data are used, an application with the DSB for the processing of sensitive data for research purposes must be accompanied by a statement signed by the person authorized to dispose of the collection of information from which the data shall be collected or by another authorized person that he/she makes available the collection of information for the research. The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.

Pursuant to section 46 (5) DSG 2000 even in those cases where the use of data in a form which permits identification of data subjects is legal for purposes of scientific research, the data shall be encrypted without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistic work can be performed with indirect personal data only. Unless expressly laid down otherwise, data in a form which permits identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistic work to keep them identifiable.

It is worth mentioning that pursuant to the DSG 2000 (further) legal restrictions on the right to make use of the data, in particular based on copyright, shall not be affected by the DSG 2000.

From which generally applicable data protection provisions are researchers exempted and under what conditions?

In Austria, section 46 DSG 2000 sets out the general regime applying to scientific research; thus, the general regime does not apply, and the researcher's (as the Controller) obligations can differ from the general Austrian data protection regime, especially when it comes to sensitive, namely health data:

Generally, section 9 DSG 2000 stipulates that the use of sensitive data does not infringe interests in secrecy deserving protection (= data protection rights) only and exclusively if (i) the data subject has obviously made public the data her-/ himself; or (ii) the data are used only in indirectly personal form; or (iii) the obligation or authorisation to use

[13] Section 4 number 1 DSG 2000 defines „indirect personal data" as data that are for the Controller, the Processor relating to the data subject in such a manner that the Controller and Processor cannot establish the identity of the data subject by legal means.

[14] Austrian Supreme Court 6 Ob 16/01 y.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the data is stipulated by laws, insofar as these serve an important public interest; or (iv) the use is made by a Controller of the public sector in fulfilment of his obligation to give inter-authority assistance; or (v) data are used that concern solely the exercise of a public office by the data subject; or (vi) the data subject has unambiguously given her/ his consent, which can be revoked at any time, the revocation making any further use of the data illegal; or (vii) the processing or transmission is in the vital interest of the data subject and his consent cannot be obtained in time; or (viii) the use is in the vital interest of a third party; or (ix) the use is necessary for establishment, exercise or defence of legal claims of the Controller before a public authority and the data were collected legitimately; or (x) data are used for scientific research or pursuant to section 46 DSG 2000; or (xi) the use is required according to the rights and duties of the Controller in the field of employment law and civil service regulations and, and is legitimate according to specific legal provisions; the rights of the labour councils according to the Austrian Labour Constitutional Act ("*Arbeitsverfassungsgesetz*") with regard to the use of data remain unaffected, or (xii) the data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care or treatment or the management of health-care services, and the use of data is performed by medical personnel or other persons subject to an equivalent duty of secrecy, or (xiii) non-profit-organisations with a political, philosophical, religious or trade-union aim process data revealing the political opinion or philosophical beliefs of natural persons in the course of their legitimate activities, as long as these are data of members, sponsors or other persons who display an interest in the aim of the organisation on a regular basis; these data shall not be disclosed to a third party without the consent of the data subjects unless otherwise provided for by law.

Furthermore, section 18 DSG 2000 stipulates that (in general) all and any data applications, which involve sensitive data may only be initiated after an examination and prior approval by the DSB.

Finally, section 27 DSG 2000 stipulates that the Controller shall erase any personal data that are processed contrary to the provisions of the DSG 2000. Section 27 DSG lays down that as soon as data are no longer needed for the purpose of the data application, they shall be regarded as illegally processed data and shall be erased unless their archiving is legally permitted and unless the access to these data is specially secured, whereas the legitimacy of further processing for scientific purposes is laid down in section 46 DSG 2000.

As described above, section 46 DSG 2000 lays down a regime (also for sensitive data) differing from the above shown general regime.

Concerning the possible exemption for scientific purposes of the general obligation to inform the data subjects see below.

c. Are there additional specific conditions governing the processing of data for scientific research purposes?

What are the suitable safeguards applied to the exemption foreseen by Article 8.4 of the Directive in your country?

The text of Article 8 (4) of the Directive requires that the processing of sensitive data, when authorised by the Member States for reasons of significant public interest, are subject to suitable safeguards. In the Austrian legal framework, processing for scientific research in the field of health is an exemption to the Directive's prohibition. However, these processing operations are governed by the provisions of section 46 DSG 2000 and section 18 DSG 2000 as described above.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Therefore, the "suitable safeguards" are (on a high level)

- generally
    - use of only "indirect personal data" (= pseudonymised data); or
    - the prior checking by and necessity of approval/ permit by the DSB;
- for scientific research
    - that data may only be used if they are (i) already publicly accessible or (ii) the Controller has already lawfully collected the data for other research projects or other purposes or (iii) the data are only indirect personal data (= pseudonymised data) for the Controller.
    - Otherwise, data not named in (i) to (iii) shall only be used under the following conditions: personal data shall only be used (a) based on specific legal provisions or (b) with the (base on Austrian case law: informed and specific) consent of the data subject or (c) with a permit of the DSB.
    - If sensitive data are to be collected/ used an important public interest in the research must exist. Furthermore, it must be ensured that the personal data is only processed by persons, who are subject to a statutory duty to confidentiality or are otherwise credible. In case third party's data are used, an application with the DSB for the processing of sensitive data for research purposes must be accompanied by a statement signed by the person authorized to dispose of the collection of information from which the data shall be collected or by another authorized person that he/she makes available the collection of information for the research. The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.
    - Pursuant to section 46 (5) DSG 2000 even in those cases where the use of data in a form which permits identification of data subjects is legal for purposes of scientific research, the data shall be encrypted without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistic work can be performed with indirect personal data only. Unless expressly laid down otherwise, data in a form which permits identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistic work to keep them identifiable.

Are there any specific provisions concerning: (i) professional secrecy, (ii) express consent for specific data, or specific provisions for (iii) deceased data subjects, or (iv) specific provisions for minors or persons subject to guardianship?

In Austria there exist numerous specific provisions concerning professional secrecy, eg the Medical Doctor Act, the Act concerning Heath Professionals, the Attorney Act, etc. Furthermore, section 15 DSG 2000 stipulates a general obligation to the Confidentiality of Data ("*Datengeheimnis*"): Controllers, Processors and people working for them, these being the employees and persons comparable to employees ("operatives"), shall keep confidential all data that have been entrusted or made accessible to them solely for professional reasons. The obligation to the Confidentiality of Data is without prejudice to other professional obligations of confidentiality. Furthermore, "operatives" may use data only if expressly ordered to do so by their employer. Controllers and Processors shall oblige their "operatives" to the above by a legal binding contract, whereas the obligation to the Confidentiality of Data shall survive even after the end of their professional relationship.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

It is worth mentioning that the DSG 2000 stipulates a criminal offence when breaching the obligation to the Confidentiality of Data; section 51 DSG 2000 reads as following: Whoever – with the intention to enrich himself or a third person unlawfully or to harm someone deliberately – illegally uses personal data that have been entrusted to or made accessible to her/ him solely because of professional reasons […] shall be punished by a criminal court with imprisonment up to a year […].

As mentioned above, pursuant to section 9 DSG 2000 the explicit and – according to the Austrian case law detailed – informed consent is one of the legal basis for the legitimate processing of sensitive data, including health data.

The DSG 2000 does not cover the protection of deceased data subjects. However, the Austrian Federal Act on the Organisation of Universities and their Studies ("*Universitätsgesetz 2002 – UG*")[15] lays down in its section 30a special provisions on the release and use of data concerning deceased persons for scientific purposes: For the purposes of medical research and analyses of deaths, the Federal Agency Statistics Austria ("*Bundesanstalt Statistik Österreich*") shall be entitled to release the date and cause of relevant deaths to scientific institutions upon agreement of the specific use of these data and against a reasonable compensation. The scientific institutions and its members shall be obliged to observe confidentiality of these data according to the Law on Statistics for Federal Purposes 2000 ("*Bundesstatistikgesetz 2000*") and shall use these data only for scientific purposes. At universities of medicine or universities with a faculty of medicine, an ethics committee shall be consulted prior to the conclusion of the agreement. At other scientific institutions, an ethics committee under the Hospitals and Health Resorts Act ("*Krankenanstalten- und Kuranstaltengesetz*") or a comparable ethics committee shall be consulted.

The DSG 2000 does not lay down special provisions for minors or persons subject to guardianship in the context of data protection.

Are there specific requirements about the data subject's information or about the person from whom the data was collected?

Section 24 DSG 2000 stipulates the Controller's general obligation to provide information to the data subjects:

The Controller shall inform the data subjects when collecting data in an appropriate manner about (i) the purpose of the data application for which for which the data are collected, and (ii) the name and address of the Controller, insofar as this as this information are not already available to the data subject with regard to the particular circumstances of the case. Further information shall be given if this is necessary for fair and lawful processing, particularly (a) if the data subject has a right to object to intended processing; or (b) if it is not clear for the data subject under the concrete circumstances whether she/ he is required by law to reply to the questions posed, or (c) data are to be processed in a joint information system ("*Informationsverbundsystem*") that is not authorised by law.

If the data have not been collected by asking the data subject, but through third sources, the above information may not be provided (aa) if the use of data is provided for by law; or (bb) if it is impossible to provide the information because the data subjects cannot be reached; or (cc) if, considering the improbability of infringements of the data subjects' rights and the expense involved in reaching the data subjects, an unreasonable effort would be required. In particular, this applies if data are collected for purposes of scientific research pursuant to section 46 DSG (see above) and the requirement to inform the data subject is not explicitly stipulated.

[15] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002128 (in German) and a bilingual version in English: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2002_1_120/ERV_2002_1_120.html.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Are there specific penalties if the conditions for processing for scientific research in the field of health purposes are not respected? What do those penalties entail?

Section 52 DSG 2000 lays down administrative penalties for certain violations of the DSG 2000: Insofar as the violation is not subject to provisions for a criminal offence or more severe penalties according to another administrative provision, an administrative offence punishable by a fine of up to 25 000 Euro is committed by anyone who intentionally uses personal data in violation of the rules on confidentiality (section 15 DSG 2000 – see details above) and in particular anybody who uses data entrusted to him according to section 46 not only for scientific purposes.

d. Formalities prior to processing: the general regime under the current framework

Is there a regime requiring the fulfilment of certain conditions prior to any processing activities?

According to section 17 DSG 2000, any use of data must be notified to the DSB for registration in the publicly accessible[16] Data Processing Register ("*Datenverarbeitungsregister – DVR*"). There are some – but in the field of scientific research not relevant – exceptions of the compulsory notification stipulated in section 17 (2) and (3) DSG 2000. Data applications (subject to notification), which involve sensitive data, such as health data, may only be initiated after an examination and prior approval by the DSB.

3. Further processing of health data (for research purposes): the current regime

As already described above, section 46 DSG 2000 allows the further processing (also) of health data for research purposes for specific projects whose goal is not to obtain results in a form relating to specific data subjects if the data has been lawfully collected by the Controller for other research projects or other purposes.

Furthermore, - if considered as "further processing" – publicly available data may be used for research projects pursuant to section 46 DSG 2000.

In this context it is worth mentioning section 27 DSG 2000: This provision stipulates that the Controller shall erase any personal data as soon as data are no longer needed for the legitimate purpose. However, the legitimacy of further processing for scientific purposes is not subject to this obligation as it is laid down in section 46 DSG 2000.

How is the notion of further processing regulated in your national framework?

The term "further processing" is not defined in the DSG 2000. However, section 4 number 12 DSG 2000 defines the term "transmission of data" ("*Übermittlung*") as "the transfer of data […], in particular […] the use of data for another

[16] https://dvr.dsb.gv.at/at.gv.bka.dvr.public/ (in German) and more specific: https://dvr.dsb.gv.at/at.gv.bka.dvr.public/DVRRecherche.aspx (in German).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

purpose of the Controller." Therefore, the term "further processing" generally falls under the term "transmission" laid down in the DSG 2000.

Pursuant to section 7 (2) DSG 2000 data shall only be transmitted if (i) they originate from a legal data application; and (ii) the recipient has satisfactorily demonstrated to the transmitting party her/ his statutory competence or legitimate authority with regard to the purpose of the transmission, insofar as it is not beyond doubt; and (iii) the interests in secrecy of the data subject deserving protection are not infringed by the purpose and content of the transmission.

Are there specific conditions to the further processing for scientific research in the field of health purposes?

Please see section 46 DSG 2000 the explanations above.

If the "further processing" is a "transmission" (see definition of the term above) between (two or more) Healthcare Providers, section 3 of the Federal Act on Data Security Measures when using personal electronic Health Data (Health Telematics Act 2012 – "*Gesundheitstelematikgesetz 2012 – GTelG 2012*") is of relevance: Healthcare Providers may disclose health information only if (i) the transfer is legitimate according to one of the purposes determined in section 9 DSG 2000, (ii) the identity of the persons whose Health Data shall be disclosed has been confirmed, (iii) the identity of the Healthcare Providers being involved in the transfer has been confirmed, (iv) the Roles of the Healthcare Providers being involved in the transfer are demonstrated, (v) the confidentiality of the shared Health Data is guaranteed and (vi) the integrity of the shared Health Data is guaranteed.

What are the rights of the data subject when it comes to further processing?

Section 1 DSG 2000 stipulates (also in case of further processing, except if only "indirect personal data" is involved) that everybody shall have the right to secrecy for her/ his personal data. Everybody shall have the right to obtain information as to who processes what data concerning her/ him, where the data originated, for which purpose they are used, as well as to whom the data are transmitted; the right to rectification of incorrect data and the right to erasure of illegally processed data.

What about the data subject's rights and further processing for scientific research purposes?

The Austrian laws do not provide special provisions on the data subject's rights and further processing for scientific research purposes. The above general regime applies.

4. The GDPR's impact on the current regulatory framework for the processing of health data for research purposes

a. The impact of the GDPR on the rules applying to processing for research in the field of health

Please provide a summary of the main relevant characteristics of the new law/Bill (as far as it is relevant for processing health data for research purposes).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Section 7 DSG (coming into force on May 25, 2018) is – by only adopting the wording to the GDPR respectively to the wording of the new DSG – a "copy" of section 46 DSG 2000 (in force until May 24, 2018), whereas the latter has already been described in detail in II.B. above.

However, currently (March 30, 2018) a draft/ bill of the Austrian Data Protection Adaptation Act for Science and Research 2018 ("*Datenschutzanpassungsgesetz Wissenschaft und Forschung 2018 – DSAP-WF*")[17] is discussed in the Austrian Parliament that would (*inter alia*) amend the Federal Act on Research Organisations in Austria ("*Forschungsorganisationsgesetz – FOG*"[18]), which would/ could be of high relevance (also) for the AEGLE project, as it would tremendously liberalise the framework:

The new FOG aims to create the conditions for "registry research" ("*Registerforschung*"), notably through the establishment of a central research database. Furthermore, it aims to ensure the operation of biobanks, to reduce bureaucratization of project authorizations and data protection impact assessments, and to remove obstacles to innovative technologies and partnerships. Furthermore, an "opt-out-register" for science and research shall be introduced, the framework conditions for knowledge and technology transfer shall be improved and ambiguities regarding the processing of personal data at the international level shall be clarified.

It is worth mentioning that the new FOG would extend the term "data" not only to "personal data" but to all data/ information.

How is (or will be) Article 9(2)(j) implemented in your country?

As mentioned above, section 7 DSG takes over the provisions of section 46 DSG 2000 that are based on Article 8 (4) of the Directive.

However, the bill of the DSAP-WF respectively of the new FOG tremendously liberalises the present regime, also in comparison to the regime of section 7 DSG (see bill of section 5 (8) FOG below):

For the purposes of the FOG, the Controllers may

- process all personal data in any case, especially in the context of Big Data, personalized medicine, biomedical research, biobanks and the transmission to Processors, if
    - instead of the name, Sector-Specific Personal-Identifier ("*bPK*") in terms of the Federal Act on Provisions Facilitating Electronic Communications with Public Bodies ("*E-Government Gesetz – E-GovG*"[19]) or other unique identifiers are used for identification; or
    - the processing takes place in a pseudonymised form (Article 4 No 5 GDPR); or
    - publications/ disclosure to the public are made
        - not at all;

[17] https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00010/ (in German).

[18] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514 (in German).

[19] Bilingual Version: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2004_1_10/ERV_2004_1_10.html.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

- only in an anonymous or pseudonymous form; or
- without name, home address and photo;

or

- the processing is done exclusively for the purpose of anonymization or pseudonymisation and there is no disclosure of personal data directly to third parties;

- obtain free of charge and within the time limit specified in article 12 (3) GDPR special bPKs from the Austrian sourcePIN Register Authority ("*Stammzahlenregisterbehörde*");
- obtain from (public) authorities, which are keeping registers, (personal) data from those registers, whereas the name must be replaced by bPKs. The authorities must provide those data in electronic format within the time mentioned in article 12 (3) GDPR and against appropriate remuneration.

Obviously to try to fulfil the requirement of "appropriate safeguards" the bill provides an "opt-out-register": Insofar as the processing of personal data for research purposes is not subject to statutory provisions, namely allowance or prohibition, data subjects may object against the procession of their data at any time ("opt-out"). The "opt-out-declaration" must specify if the "opt-out" refers to specific projects or is a "general opt-out declaration". A "general opt-out declaration" may be declared (i) in writing to the Austrian sourcePIN Register Authority ("*Stammzahlenregisterbehörde*") or (ii) electronically by way of registration with the "Opt-Out-Register" to be established and run by the Austrian sourcePIN Register Authority ("*Stammzahlenregisterbehörde*"). The "opt-out-entrance" shall be kept in the "Opt-Out-Register" until it is withdrawn or until the death of the data subject. For the determination of the time of death of the data subject, the Federal Institute for Statistics Austria ("*Bundesanstalt Statistik Österreich*") shall provide the Austrian sourcePIN Register Authority ("*Stammzahlenregisterbehörde*") at least once a month with the death dates linked to bKPs. The Austrian sourcePIN Register Authority ("*Stammzahlenregisterbehörde*") must provide upon request to Scientific Facilities and against the provision of the regarding bKPs the information on the extent of the "opt-out-declarations" via an electronic interface free of charge.

The bill of the new FOG would also introduce the (new) possibility of obtaining a "broad consent": Section 5 (4) FOG would stipulate that when obtaining consent (article 4 No. 11 GDPR) the indication of a purpose is not required. Instead, the indication of the following would be sufficient: (i) a research area; or (ii) several research areas; or (iii) research projects; or (iv) parts of research projects.

Furthermore, section 5 (5) FOG would clarify that "further processing" pursuant to Article 5 (1) (b) GDPR for purposes in terms of Article 89 GDPR are not inadmissible.

Section 5 (6) FOG would lay down that pursuant to article 5 (1) (e) GDPR, personal data may be stored for purposes specified in Article 89 GDPR without restriction if the FOG does not provide for time limits for storage.

The following data subject rights would not apply pursuant to section 5 (7) FOG if the purpose pursuant to Article 89 GDPR is likely made impossible or seriously impaired:

- Right to access by the data subject (Article 15 GDPR);
- Right to rectification (Article 16 GDPR);
- Right to erasure (Article 17 GDPR);

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

- Right to restriction of processing (Article 18 GDPR);
- Right to data portability (Article 20 GDPR); as well as
- Right of object (Article 21 GDPR).

Pursuant to the bill of section 5 (8) FOG (and by way of explicit derogation from section 7 DSG – see above concerning the identical regulations in section 46 DSG 2000), within the scope of the FOG the obtaining of a permit by the DSB is not necessary and can personal data be processed even without (a) a specific statutory provision (section 7 (2) No 1 DSG = section 46 (2) No 1 DSG 2000); or (b) a consent of the data subject (section 7 (2) No 2 DSG = section 46 (2) No 2 DSG 2000); or (c) the voluntary confirmation by the DSB (see below), as far as the requirements of section 7 (3) DSG are met. Those are (aa) the consent of the data subject is impossible to obtain because the data subject cannot be reached or the effort would otherwise be unreasonable; (bb) there is a public interest in the processing, and (cc) the professional aptitude of the Controller is beyond doubt. However, if special categories of personal data (Article 9 GDPR) are to be collected, an important public interest in the research project must exist; furthermore, it must be ensured that the personal data are processed at the premises of the Controller ordering the research project only by persons who are subject to a statutory obligation of confidentiality regarding the subject matter of the research project or whose reliability in this respect is credible. Scientific Institutions have the right to request a voluntary confirmation by the DSB on the existence of these conditions.

Pursuant to the bill of section 5 (9) FOG (and by way of explicit derogation of section 12 (4) No 3 and No 4 DSG) within the scope of the FOG and/ or the scope of section 44 of the Health and Nursing Act the automation-supported matching of personal data obtained by taking pictures with personal data, including special categories of personal data (Article 9 GDPR) as a selection criterion, is legitimate for purposes pursuant to Article 89 GDPR provided that (i) the processing is carried out by scientific institutions and (ii) there is no publication/ disclosure of personal data.

Pursuant to the bill of section 9 (1) FOG Scientific Institutions may use research material for purposes pursuant to article 89 GDPR, in particular collect, archive and systematically store all data that are required to ensure optimal access to data and to ensure research material for purposes according to Article 89 GDPR ("Repositories").

b. Modification to the processing authorisation procedure applying to research in the field of health

As already described above, pursuant to the bill of section 5 (8) FOG within the scope of the FOG the obtaining of a permit by the DSB is not necessary.

Therefore, personal health data can be processed within the scope of the FOG even without (a) a specific statutory provision; or (b) a consent of the data subject; or (c) the permit and/ or voluntary confirmation by the DSB, as far as the requirements of section 7 (3) DSG are met. Those are (aa) the consent of the data subject is impossible to obtain because the data subject cannot be reached or the effort would otherwise be unreasonable; (bb) there is a public interest in the processing, and (cc) the professional aptitude of the Controller is beyond doubt. However, if health data are to be processed, an important public interest in the research project must exist; furthermore, it must be ensured that the personal data are processed at the premises of the Controller ordering the research project only by persons who are subject to a statutory obligation of confidentiality regarding the subject matter of the research project or whose reliability in this respect is credible.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

What about the right of the data subject and the obligations of the controller?

The bill for a new FOG provides for an "opt-out-register": Insofar as the processing of personal data for research purposes is not subject to statutory provisions, namely allowance or prohibition, data subjects may object against the procession of their data at any time ("opt-out").

However, if the data subject is subject to a processing pursuant to Article 89 GDPR and the data subject's rights would likely make it impossible or would seriously impair the purpose the right to access by the data subject (Article 15 GDPR); the right to rectification (Article 16 GDPR); the right to erasure (Article 17 GDPR); the right to restriction of processing (Article 18 GDPR); the right to data portability (Article 20 GDPR); and/ or the right of object (Article 21 GDPR) does/ do not exist.

5. Further processing for research purposes under the GDPR

Given the regime applied to further processing in the GDPR, can you describe the consequences, if any, in your national legal framework?

As described under III above, the Austrian regime under the current DSG 2000 for "further processing", namely "transmission", is very strict and has been applied by the Austrian case law even in a stricter manner. Therefore, in Austria in fact a very strong "purpose limitation" has been applied until today.

Consequently, in Austria the GDPR will lead to a liberalised approach towards the "further processing".

Pursuant to the above presented bill of the new FOG the approach towards the "further processing" for research purposes would tremendously be liberalised in comparison to the present regime.

6. Health data sources for research purposes

a. Sources of data and their regulation

Does your national framework contain specific provisions for anonymised or pseudonymised health data?

There are currently no specific provisions for anonymised or pseudonymised health data in Austria.

However, pursuant to section 46 (5) DSG 2000 even in those cases where the use of data in a form which permits identification of data subjects is legal for purposes of scientific research, the data shall be encrypted without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistic work can be performed with indirect personal data only. Unless expressly laid down otherwise, data in a form which permits identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistic work to keep them identifiable.

In the bill for the revised legal framework, the new Article 5 (I) lit d FOG states that processing of personal data especially in the context of Big Data, biobanks, personalized medicine and biomedical research is allowed for the

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

purpose of anonymization or pseudonymisation, providing that there is no disclosure of personal data to third persons during the process.

What are the different sources of health data that can be used for research purposes?

- **DIRECT COLLECTION FROM PATIENTS:**

Under the current legal framework: please explain the currently applying rules that a researcher, who intends to collect health data directly from individuals (e.g. via a survey, or by asking patients to wear a monitoring device, etc.), should follow.

The question can only be answered by distinguishing two cases:

- If the researcher is able to obtain the explicit and informed consent by the data subject, obtaining this consent is the only way under the current legal framework for a researcher to collect health data directly from individuals (e.g. via a survey, or by asking patients to wear a monitoring device, etc.).

- However, if the researcher is not in the position to obtain the explicit consent, because those data subjects cannot be reached or the effort would otherwise be unreasonable; and there is an important public interest in the use of the personal data; and the professional aptitude of the researcher has satisfactorily been demonstrated to the DSB, the researcher can apply for a permit by the DSB. Furthermore, it must be ensured that the personal data is only processed by persons, who are subject to a statutory duty to confidentiality or are otherwise credible. The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.

Furthermore, and in both cases, the researcher must under the current regime apply for a prior approval by the DSB for the processing of the personal health data.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

This would change if the bill of the FOG comes into force: Then personal health data could be processed within the scope of the FOG even without (a) a specific statutory provision; or (b) a consent by the data subject; or (c) the permit and/ or voluntary confirmation by the DSB, as far as the requirements of section 7 (3) DSG are met. Those are (aa) the consent of the data subject is impossible to obtain because the data subject cannot be reached or the effort would otherwise be unreasonable; (bb) there is an important public interest in the processing, and (cc) the professional aptitude of the Controller is beyond doubt; furthermore, it must be ensured that the personal data are processed at the premises of the Controller ordering the research project only by persons who are subject to a statutory obligation of confidentiality regarding the subject matter of the research project or whose reliability in this respect is credible.

Pursuant to the bill the new FOG also the (new) possibility of obtaining a "broad consent" would be introduced: Section 5 (4) FOG would stipulate that when obtaining consent (article 4 No. 11 GDPR) the indication of a purpose is not required. Instead, the indication of the following would be sufficient: (i) a research area; or (ii) several research areas; or (iii) research projects; or (iv) parts of research projects.

Furthermore, no prior approval by the DSB must be obtained anymore.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

- **COLLECTION FROM HEALTH PROFESSIONALS AND HEALTH INSTITUTIONS**

Under the current legal framework: please explain the rules currently applying that a researcher, who intends to obtain health data from medical staff, hospitals, etc., should follow.

It must be distinguished between three categories of use of personal health data for the purpose of scientific research and obtaining health data from medical staff, hospitals, etc., namely

i. for the purpose of specific scientific research projects whose goal is not to obtain results in a form relating to specific data subjects,

ii. research projects that are not specific, but whose goal is not to obtain results in a form relating to specific data subjects, and

iii. those projects whose goal is to obtain results in a form relating to specific data subjects.

Concerning i. specific projects whose goal is not to obtain results in a form relating to specific data subjects the researcher has the right to collect and to use all data that are for the researcher only indirect personal data (= pseudonymised data).

For ii. projects that are not specific or iii. whose goal is to obtain results in a form relating to specific data subjects any personal data shall only be used (a) based on specific legal provisions or (b) with the (based on Austrian case law: informed and specific) consent of the data subject or (c) with a permit of the DSB. Therefore, a permit by the DSB can substitute the general requirements of (a) a specific legal provision or (b) the consent of the data subject. A permit must be granted by the DSB for the use of personal health data for purposes of scientific research upon request by the researcher if (aa) the consent of the data subjects is impossible to be obtained, because those data subjects cannot be reached or the effort would otherwise be unreasonable; and (bb) there is an important public interest in the use of the personal data; and (cc) the professional aptitude of the researcher has satisfactorily been demonstrated to the DSB. Furthermore, it must be ensured that the personal data is only processed by persons, who are subject to a statutory duty to confidentiality or are otherwise credible.

As third party's data – namely collected by medical staff, hospitals, etc. – are used, an application with the DSB for the processing of health data for research purposes must be accompanied by a statement signed by the person authorized to dispose of the collection of information from which the data shall be collected or by another authorized person that he/she makes available the collection of information for the research.

The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Although section 7 DSG (coming into force on May 25, 2018) is – by only adopting the wording to the GDPR respectively the wording of the new DSG – a copy of section 46 DSG 2000 (in force until May 24, 2018), the current (March 30, 2018) draft/ bill of the Austrian Data Protection Adaptation Act for Science and Research 2018 ("*Datenschutzanpassungsgesetz Wissenschaft und Forschung 2018 – DSAP-WF*") *inter alia* amending the Federal Act

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

on Research Organisations in Austria ("*Forschungsorganisationsgesetz – FOG*") would tremendously liberalise the current framework:

The researcher may

- process all personal data in any case, especially in the context of Big Data, personalized medicine, biomedical research, biobanks and the transmission to Processors, if
    - instead of the name, Sector-Specific Personal-Identifier ("*bPK*") in terms of the Federal Act on Provisions Facilitating Electronic Communications with Public Bodies ("*E-Government Gesetz – E-GovG*") or other unique identifiers are used for identification; or
    - the processing takes place in a pseudonymised form (Article 4 No 5 GDPR); or
    - publications/ disclosure to the public are made
        - not at all;
        - only in an anonymous or pseudonymous form; or
        - without name, home address and photo;

or

- the processing is done exclusively for the purpose of anonymisation or pseudonymisation and there is no disclosure of personal data directly to third parties.

Furthermore, section 5 (5) FOG would clarify that "further processing" pursuant to Article 5 (1) (b) GDPR for purposes in terms of Article 89 GDPR are not inadmissible.

Pursuant to the bill of section 5 (8) FOG (and by way of explicit derogation from section 7 DSG – see above concerning the identical regulations in section 46 DSG 2000), within the scope of the FOG the obtaining of a permit by the DSB is not necessary and can personal data be processed even without (a) a specific statutory provision; or (b) a consent of the data subject; or (c) the permit/ the voluntary confirmation by the DSB, as far as the requirements of section 7 (3) DSG are met. Those are (aa) the consent of the data subject is impossible to obtain because the data subject cannot be reached or the effort would otherwise be unreasonable; (bb) there is an important public interest in the processing, and (cc) the professional aptitude of the Controller is beyond doubt. Furthermore, it must be ensured that the personal data are processed at the premises of the researcher ordering the research project only by persons who are subject to a statutory obligation of confidentiality regarding the subject matter of the research project or whose reliability in this respect is credible.

Pursuant to the bill of section 9 (1) FOG Scientific Institutions may use research material for purposes pursuant to article 89 GDPR, in particular collect, archive and systematically store all data that are required to ensure optimal access to data and to ensure research material for purposes according to Article 89 GDPR ("Repositories").

If the requirements of the FOG are met, no data protection impact assessment in terms of Art 35 GDPR must be accomplished.

- **PRIVATE DATABASES**

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Under the current legal framework: please explain the rules currently applying for the setting up of and the use of a private database with health data for research purposes.

Currently, there are no special provisions for the setting up of and the use of a private database with health data for research purposes in Austria. Consequently, the general rules apply:

Such database for scientific research may include data that are (i) already publicly accessible; or (ii) the Controller has already lawfully collected the data for other research projects or other purposes; or (iii) the data are only indirect personal data (= pseudonymised data) for the Controller. Otherwise, such databases may only be set up (a) based on specific legal provisions; or (b) with the (based on Austrian case law[20]: informed and specific) consent of the data subject; or (c) with a permit of the DSB, which seems difficult to obtain, as *inter alia* an important public interest in the research must exist and in case third party's data are used, an application with the DSB for the processing of sensitive data for research purposes must be accompanied by a statement signed by the person authorized to dispose of the collection of information from which the data shall be collected or by another authorized person that he/she makes available the collection of information for the research. The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.

Furthermore, such databases must overcome section 46 (5) DSG 2000: Even in those cases where the use of data in a form which permits identification of data subjects is legal for purposes of scientific research, the data shall be encrypted without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistic work can be performed with indirect personal data only. Unless expressly laid down otherwise, data in a form which permits identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistic work to keep them identifiable.

Furthermore, section 18 DSG 2000 stipulates that such database containing health data may only be initiated after an examination and prior approval by the DSB.

The Controller shall inform the data subjects when collecting data in an appropriate manner about (i) the purpose of the data application for which for which the data are collected, and (ii) the name and address of the Controller, insofar as this as this information are not already available to the data subject with regard to the particular circumstances of the case. Further information shall be given if this is necessary for fair and lawful processing, particularly (a) if the data subject has a right to object to intended processing; or (b) if it is not clear for the data subject under the concrete circumstances whether she/ he is required by law to reply to the questions posed, or (c) data are to be processed in a joint information system ("*Informationsverbundsystem*") that is not authorised by law.

If the data have not been collected by asking the data subject, but through third sources, the above information may not be provided (aa) if the use of data is provided for by law; or (bb) if it is impossible to provide the information because the data subjects cannot be reached; or (cc) if, considering the improbability of infringements of the data subjects' rights and the expense involved in reaching the data subjects, an unreasonable effort would be required. In particular, this applies if data are collected for purposes of scientific research and the requirement to inform the data subject is not explicitly stipulated.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

[20] Austrian Supreme Court 6 Ob 16/01 y.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Pursuant to the bill of section 9 (1) FOG Scientific Institutions may use research material for purposes pursuant to article 89 GDPR, in particular collect, archive and systematically store all data that are required to ensure optimal access to data and to ensure research material for purposes according to Article 89 GDPR ("Repositories").

"Scientific Institutions" are defined in the bill as “natural persons, communities of persons as well as legal persons pursuing purposes pursuant to article 89 (1) GDPR, regardless of whether this is for charitable purposes (sections 34 et sqq of the Federal Tax Code) or not or at university or non-university level. Therefore, databases by private Scientific Institutions would be covered by section 9 FOG.

- **PUBLIC DATABASES**

Under the current legal framework: do public authorities make available health data for research purposes in your country and under what conditions?

There are a handful of public databases in Austria, providing/ referring to health data, eg:

- Statistik Austria (http://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/gesundheit/index.html);
- Genom Austria (http://genomaustria.at);
- NIS datenbank from AGES (https://forms.ages.at/nis/listNis.do);
- Gesundheit Österreich GmbH (https://goeg.at/).

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Pursuant to the bill of section 9 (1) FOG Scientific Institutions may use research material for purposes pursuant to article 89 GDPR, in particular collect, archive and systematically store all data that are required to ensure optimal access to data and to ensure research material for purposes according to Article 89 GDPR ("Repositories").

"Scientific Institutions" are defined in the bill as “natural persons, communities of persons as well as legal persons pursuing purposes pursuant to article 89 (1) GDPR, regardless of whether this is for charitable purposes (sections 34 et sqq of the Federal Tax Code) or not or at university or non-university level. Therefore, databases by private Scientific Institutions would be covered by section 9 FOG.

b. Application of the national framework to the AEGLE cases

In the AEGLE project, the “research objective is to establish the use of Big data analysis in the prediction of outcomes in three working scenarios: Chronic Lymphotic Leukemia (CLL), Intensive Care Units and type 2 diabetes for the prediction of adverse outcomes. The research methodology is Big Data analysis to establish predictive values that may apply in three clinical scenarios and to see if this can be generalised to other healthcare disease models”. [21]

[21] AEGLE Grant Agreement, Annex 1, p. 83.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

To achieve its objective, the AEGLE project must base its approach on the study, and thus the processing, of data concerning health. This section aims to address each of the three proposed AEGLE cases, and to determine the requirements in general terms for access and the processes relevant to data under the Directive (the current framework) and the GDPR.

1. Type 2 diabetes

The AEGLE project uses, after pseudonymisation, existing databases with health data collected from patients who expressed their consent to their data being used for research purposes.

Under the current Austrian legal framework:

Assuming that an explicit and informed consent has been given by the patients to pseudonymise their data (as this is a "further processing" = "transmission" under the DSG 2000) the use of the pseudonymised data in the existing databases is legitimate. As section 9 DSG 2000 stipulates that the use of sensitive data (= health data) does not infringe interests in secrecy if the data are used in an indirect personal form (= pseudonymised data), the "further processing" of the pseudonymised health data in the AEGLE project "Type 2 diabetes" is legitimate and no notification to and no prior approval by the DSB is necessary.

Furthermore, as only "indirect personal data" is processed in the AEGLE project "Type 2 diabetes" the DSG 2000 does no grant any data subjects' rights (section 29 DSG 2000) and no information obligation exists (section 24 (4) DSG 2000 in connection with section 17 (2) DSG 2000).

Under the (possible) future Austrian legal framework:

Pursuant to the GDPR and the DSG generally the legal framework is also applicable on pseudonymised data. However, section 7 DSG stipulates that for scientific research purposes, whose goal is not to obtain results in a form relating to specific data subjects, the Controller may process all personal data that are pseudonymised personal data and the identity of the data subject cannot be establish by legal means.

The bill of the new FOG would additionally introduce the (new) possibility of obtaining a "broad consent": Section 5 (4) FOG would stipulate that when obtaining consent (article 4 No. 11 GDPR) the indication of a purpose is not required. Instead, the indication of the following would be sufficient: (i) a research area; or (ii) several research areas; or (iii) research projects; or (iv) parts of research projects. Therefore, the "further processing" for the AEGLE project "Type 2 diabetes" could be covered by such "broad consent". Furthermore, section 5 (5) FOG would clarify that "further processing" pursuant to Article 5 (1) (b) GDPR for purposes in terms of Article 89 GDPR are not inadmissible.

On the other hand, the bill of the new FOG stipulates that the processing for the purpose of anonymisation or pseudonymisation without any disclosure of personal data directly to third parties is – also without the data subjects' consent – legitimate. Therefore, the patients' consent for the pseudonymisation would not be required in the first place. Furthermore, pursuant to the bill of the new FOG for the purposes of the FOG, the Controller may process all personal data in any case, especially in the context of Big Data, personalized medicine, biomedical research, biobanks and the transmission to Processors, if the processing takes place in a pseudonymised form (Article 4 No 5 GDPR). Therefore, the "further processing" for the AEGLE project "Type 2 diabetes" could (also) be covered by processing of the health data in a pseudonymised form.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

And the following data subject rights would not apply pursuant to section 5 (7) FOG if the purpose pursuant to Article 89 GDPR is likely made impossible or seriously impaired:

- Right to access by the data subject (Article 15 GDPR);
- Right to rectification (Article 16 GDPR);
- Right to erasure (Article 17 GDPR);
- Right to restriction of processing (Article 18 GDPR);
- Right to data portability (Article 20 GDPR); as well as
- Right of object (Article 21 GDPR).

Nevertheless, the further obligations of the Controller (and the Processor) under the GDPR (however, pursuant to the FOG no data protection impact assessment in terms of Art 35 GDPR) and the DSG must be met.

The above applies (concerning the bill would apply) on the AEGLE project "Type 2 diabetes".

2. Intensive Care Unit (ICU)

AEGLE uses data generated by ICU devices without collecting the patient's consent, however after pseudonymisation.

Under the current Austrian legal framework:

As no explicit and informed consent for the pseudonymisation of the patients' data (as this is a "further processing" = "transmission" under the DSG 2000) exists, the collecting of the data generated by the ICU devices and the pseudonymisation and further processing in the AEGLE project "ICU" is subject to section 46 DSG 2000: Consequently, for the collection of the data via the ICU devices the permit of the DSB is required.

However, a permit must be granted by the DSB for the use of personal data for the AEGLE project "ICU" upon request only if (aa) the consent of the data subjects is impossible to be obtained, because those data subjects cannot be reached or the effort would otherwise be unreasonable; and (bb) there is an important public interest in the use of the personal data; and (cc) the professional aptitude of the applicant/ the Controller has satisfactorily been demonstrated to the DSB. Furthermore, it must be ensured that the personal data is only processed regarding the ICU devices by persons, who are subject to a statutory duty to confidentiality or are otherwise credible.

In case third party's data are used (e.g. third-party ICU devices), an application with the DSB for the processing must be accompanied by a statement signed by the person authorized to dispose of the ICU device data.

The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.

However, as then in the actual AEGLE project "ICU" only "indirect personal data" (= pseudonymised data) are processed, no notification of and no prior approval by the DSB is necessary for this "further processing". Furthermore, as only "indirect personal data" is processed in the actual AEGLE project "ICU" the DSG 2000 does no

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

grant the data subjects' rights (section 29 DSG 2000) and no information obligation exists (section 24 (4) DSG 2000 in connection with section 17 (2) DSG 2000).

Under the (possible) future Austrian legal framework:

As no explicit and informed consent for the pseudonymisation of the patients' data exists, the collecting of the data generated by the ICU devices and the pseudonymisation and further processing in the AEGLE project "ICU" is subject to section 7 DSG (= same proceeding as described for section 46 DSG 2000 above).

However, the bill of the new FOG stipulates that the processing for the purpose of anonymisation or pseudonymisation without any disclosure of personal data directly to third parties is – also without the data subjects' consent – legitimate. Therefore, the patients' consent for the pseudonymisation would not be required. Furthermore, pursuant to the bill of the new FOG for the purposes of the FOG, the Controller may process all personal data in any case, especially in the context of Big Data, personalized medicine, biomedical research, biobanks and the transmission to Processors, if the processing takes place in a pseudonymised form (Article 4 No 5 GDPR). And the following data subject rights would not apply pursuant to section 5 (7) FOG if the purpose pursuant to Article 89 GDPR is likely made impossible or seriously impaired:

- Right to access by the data subject (Article 15 GDPR);
- Right to rectification (Article 16 GDPR);
- Right to erasure (Article 17 GDPR);
- Right to restriction of processing (Article 18 GDPR);
- Right to data portability (Article 20 GDPR); as well as
- Right of object (Article 21 GDPR).

Nevertheless, the further obligations of the Controller (and the Processor) under the GDPR (however, pursuant to the FOG no data protection impact assessment in terms of Art 35 GDPR) and the DSG must be met by the AEGLE project "ICU".

3. Chronic Lymphocytic Leukemia (CLL)

The AEGLE project re-uses, after pseudonymisation, data coming from biobanks. In this instance, patients have given their informed consent for the samples and for the processing of their data. But this consent was given in general terms and not specifically for AEGLE.

Under the current Austrian legal framework:

As the pseudonymisation of the patients' data for the use in the AEGLE project "CCL" is not covered by the patients' "broad consent" – as such "broad consent" does not exist under the current regime – section 46 DSG 2000 applies: Consequently, for the pseudonymisation of the patients' data for the use in the AEGLE project "CCL" the permit of the DSB is required.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

A permit must only be granted by the DSB for the pseudonymisation of the patients' data for the use in the AEGLE project "CCL" if (aa) the consent of the data subjects is impossible to be obtained, because those data subjects cannot be reached or the effort would otherwise be unreasonable; and (bb) there is an important public interest in the use of the personal data; and (cc) the professional aptitude of the applicant/ the Controller has satisfactorily been demonstrated to the DSB. As third party's data, namely those of biobanks, are used, an application with the DSB for the processing with in the AEGLE project "CCL" must be accompanied by a statement signed by the person authorized by the biobanks. The DSB may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests.

As then in the actual AEGLE project "CLL" only "indirect personal data" (= pseudonymised data) are processed no notification of the DSB is necessary for this "further processing". Furthermore, as only "indirect personal data" is processed the DSG 2000 does no grant the data subjects' rights (section 29 DSG 2000) and no information obligation exists (section 24 (4) DSG 2000 in connection with section 17 (2) DSG 2000).

Under the (possible) future Austrian legal framework:

The bill of the new FOG would introduce the (new) possibility of obtaining a "broad consent": Section 5 (4) FOG would stipulate that when obtaining consent (article 4 No. 11 GDPR) the indication of a purpose is not required. Instead, the indication of the following would be sufficient: (i) a research area; or (ii) several research areas; or (iii) research projects; or (iv) parts of research projects. Therefore, the "further processing" for the AEGLE project "CLL" would be covered by the "broad consent". Furthermore, section 5 (5) FOG would clarify that "further processing" pursuant to Article 5 (1) (b) GDPR for purposes in terms of Article 89 GDPR are not inadmissible.

The following data subject rights would not apply pursuant to section 5 (7) FOG if the purpose pursuant to Article 89 GDPR is likely made impossible or seriously impaired:

- Right to access by the data subject (Article 15 GDPR);
- Right to rectification (Article 16 GDPR);
- Right to erasure (Article 17 GDPR);
- Right to restriction of processing (Article 18 GDPR);
- Right to data portability (Article 20 GDPR); as well as
- Right of object (Article 21 GDPR).

Nevertheless, the further obligations of the Controller (and the Processor) under the GDPR (however, pursuant to the FOG no data protection impact assessment in terms of Art 35 GDPR) and the DSG must be met by the AEGLE project "CLL".

GEISTWERT, Vienna, March 30, 2018, updated July 2018

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU