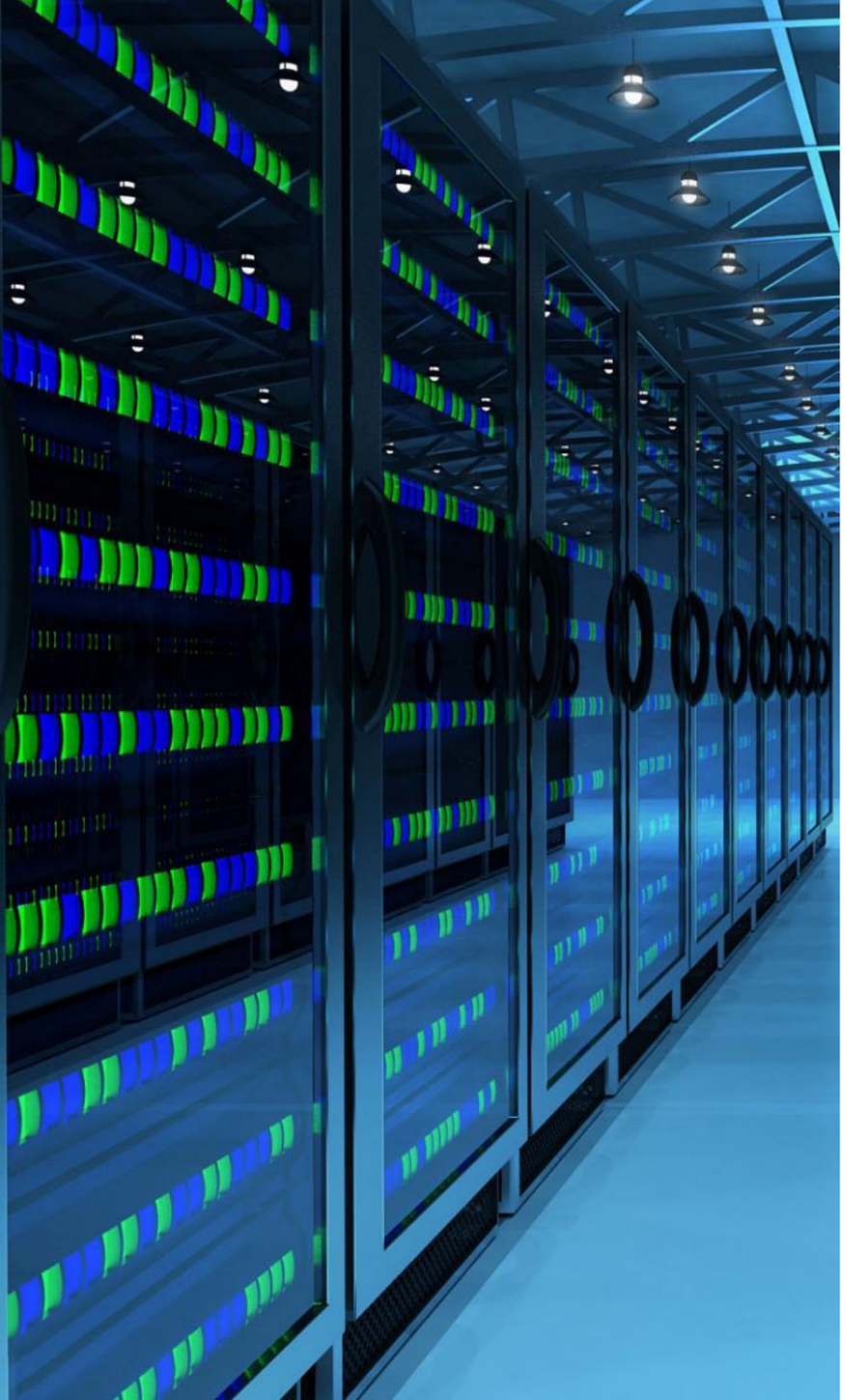
TaylorWessing

Personalized Medicine, Privacy and Data-related Issues

SINO-EU PerMed Seminar Florence

17.2.2022 | Dr. Thomas Pattloch

Content



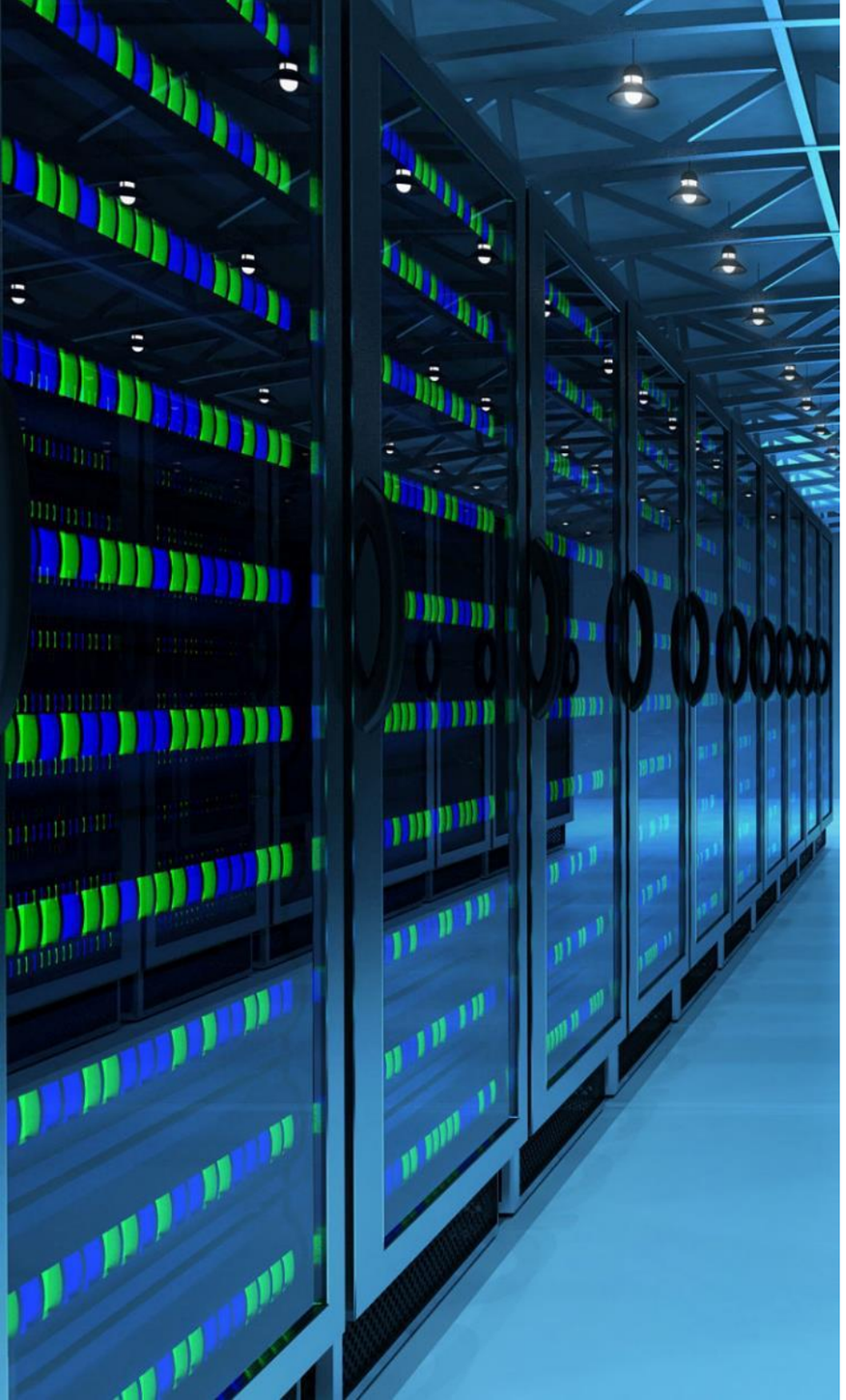
1 | Case example

TaylorWessing

Cross-border hospital cooperation on cancer-related research with patient studies

A German research institute with adjunct hospitals plans to support the set-up of a clinic and adjunct research institute on cancer diseases in China. The Chinese partner, a well-known university with affiliates, would like to invite scholars and researchers for research stays in China to set-up and structure the research, and to develop new treatments for patients based on personalized medicines. German visiting physicians shall create and supervise the treatment of own selected patient groups, shall collect data arising out of the treatment and use it for development of new APIs, but also for commercialization including patent filing. Some other data shall be published for research.

- Research results are jointly generated with Chinese researchers, and data on patients and their treatment shall be sent via Email and other channels to each other cross-border. It is yet unclear whether data can be pseudonimized to full extent, or which data will or has to be in its original state.
- The data is stored on servers on the premises of the Chinese partner and its hospital, but also on servers in Germany of the German research institute once received. Users of data ultimately will be also third parties, but only after it is pseudonimized.
- To what extent is such cooperation is subject to special GDPR requirements and how can these requirements be met?



2 | Typical legal issues for physicians

Gene diagnostics

Key element for “personalized medicine“: Analysis of cancer etc. develops into many sub-branches of diseases, making identification of individual patients more/highly likely

- Reactive treatment
- Preventive treatment, e.g. § 3 No. 8 GenDG

Challenge for physicians of having to apply the correct standard of care, otherwise risk of infringement of treatment contract with patient – means identification of patient data and use of it, e.g. by laboratories

- Standard of care may require conducting pre-tests
- Guidelines of the Gene Diagnostics Commission (GEKO): Established in § 23 para. 2 GenDG the task of filling in and specifying numerous terms of the GenDG in these guidelines.

Guidelines for treatment become increasingly less “standard” with more personalized medicine

Pharmacological safety of drugs and treatment requires more data than what is often available, groups of patients treated shrink

Requirements under local laws, e.g. German law

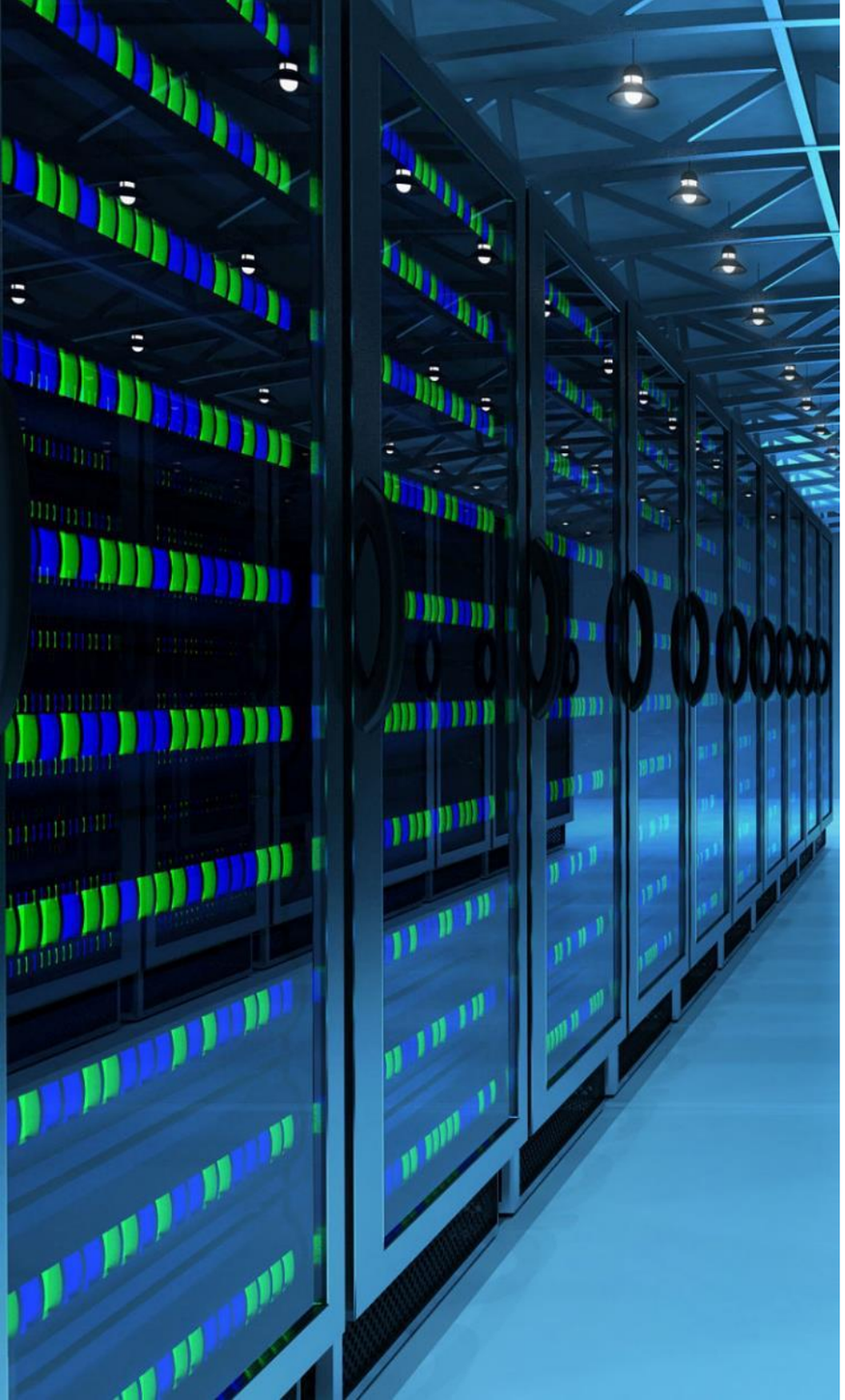
- Impact on civil treatment contract with patient, §§ 630a et seq. German Civil Code BGB
- Reimbursement of costs may depend on proper adherence to necessary pre-testing
- Gendiagnostikgesetz GenDG – German Gene Diagnostics Act; for some preimplantation genetic diagnosis other laws such as the Embryo Protection Act
- In case of sensitive personal data use of third parties could lead to breach of professional secrecy and liability under criminal code

Privacy

Protecting the dignity and the right of self-determination of the persons concerned is the primary objective of the Gene Diagnostics Act.

However, the requirements for legal compliance for proper information, consent and genetic counseling are extremely demanding:

- Consent required by patient, § 8 para. 1 GenDG, separately from extraction and examination, and must specify the scope of the examination
- Information of patient in advance of tests puts high requirements, see GEKO guidelines § 23 para 2 No. 3 GenDG, and requires documentation and time to consider for patients to withdraw consent
- Information must be made by specifically qualified physician
- Consent must be specific, in writing, and to the responsible physician; breach of obligations may result into liability of physician
- Consent must encompass scope of genetic testing, patient may limit such scope (§ 8 para. 1 sent. 2 GenDG), and may include instruction by patients on what shall happen with the test results (partial of full destruction)
- Physicians must deal with possibility that consent is withdrawn



3 | Data protection, privacy

TaylorWessing

Genetic/biometric/health data in the GDPR

- Definitions in Art. 4 (13)-(15) GDPR
- General lawfulness of processing subject to Art. 6 GDPR, including inter alia informed consent (purpose-bound!), or contract, legal obligations of controller, vital interests of data subject
- Art. 9 para 1 special category of personal data requires exemption under para 2 for processing
- EU member states may add additional conditions for the processing of such data (§ 9 para 4 GDPR), e.g. Germany with the Gene Diagnostics Act which requires written form as additional requirement for processing
- Art 9 para 2 lit. g)-j) may be applicable exemptions:
  - Processing for substantial public interest
  - Processing necessary for the purposes of preventive or occupational medicine,…, medical diagnosis, the provision of health or social care…the provision of health treatment… or management of health care systems and services… or pursuant to contract with a health professional… subject to … para 3.
  - Processing necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products and medical devices
  - Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Consent in research, recital 33 and “broad consent”

- Because many questions are not even determined at the beginning of a research project, the data subject should therefore be able to declare consent "for certain research areas or parts of research projects to the extent permitted by the purpose pursued".
- The German Data Protection Commission (DSK) also recognizes broad consent, taking into account certain corrective measures to ensure transparency, trust and data security in certain individual cases, if the concrete design of the research project foreseeably does not permit a complete definition of the purpose per se until the time of data collection.
  - Discussion on “informed consent”, “dynamic consent” and “meta consent” instead
  - What is “data donation” – does it exclude withdrawal of consent?

Art. 9 j in conjunction with Art. 89 para 1 GDPR

"1. Processing for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, shall be **subject to appropriate safeguards**, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure **respect for the principle of data minimization**. Those measures may include **pseudonymisation** provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

Processing of health, biometric and genetic data also for purposes of Art. 89 is only permissible if there is a legal basis for this in EU or national law (see recital No. 53):

- Member States may introduce or maintain further restrictions on the processing of genetic, biometric or health data pursuant to Art. 9(4) GDPR, which, however, must not impair the free movement of data within the EU.
- Consent of data subject cannot abrogate technical and organizational measures (in particular, but not limited to data minimization through pseudonymisation), measures must exist and accord to standards required under GDPR
- Recital 156 provides that the processing of personal data for the purposes specified in Art. 89 may only take place after the controller has examined whether it is possible to fulfill these purposes by processing anonymized or pseudonymized data.

Narrow or wide interpretation e.g. of “research for scientific purposes”

- Decisive factor for a privileged status as science is the goal of transparent knowledge generation for the general public?
- This must be distinguished from commercially motivated research projects
  - Privileged treatment of privately financed research can therefore only be considered if the **core characteristics of scientific research are also fulfilled: the transparency of the research process and the results, the independence and autonomy of the researchers, and the goal of gaining knowledge in the general interest free of extraneous considerations?**
- Criteria also relevant for the classification of traditional third-party funded research at universities?

Art. 89 para 2 GDPR

"2. Where **personal data are processed for scientific** or historical **research purposes** or statistical purposes, Union or Member State law **may provide for derogations from the rights** referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article **in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes**."

In practice, in the case of mixed-funded or partly commercial research projects, the pure research activity and the publication of the results in the interest of the general public may or may not fall under the scope of application of Art. 89, while a subsequent use of the research results for corporate purposes will no longer be subject to the privileges of the GDPR and will require its own legal basis, either in the form of the consent of the data subjects or by means of a special legal permission norm.

Art. 21 para 6 GDPR: "6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation**, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest**."

Consequently, a distinction must be made in principle: On the one hand, data may be released for research purposes by means of an informed (broad) consent of the data subject, which may be revoked. The data must be deleted as a result of a revocation, unless there is another legal basis for the (further) processing. On the other hand, data processing may be based on a legal basis from the outset. An objection by the data subject can apply, which in turn can be limited in its scope.

National law may allow research exemption, e.g. § 27 BDSG German law

Exemption requires specific measures for protection of data subject:

- technical organizational measures,
- measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered, modified or removed,
- sensitization of those involved in processing operations,
- designation of a data protection officer,
- Restricting access to personal data within the controller and by processors,
- pseudonymization of personal data,
- encryption of personal data,
- ensuring the capability, confidentiality, integrity, availability and resilience of the systems and services related to the processing,
- to ensure the security of processing, the establishment of a procedure for periodic review, assessment and evaluation of the effectiveness of technical and organizational measures; or
- **specific procedural arrangements to ensure compliance with the requirements of the BDSG and Regulation (EU) 2016/679 in the event of transfer or processing for other purposes**.

Additional requirement: Art. 35 GDPR– see also Art. 55 Chinese Personal Information Protection Law Data Protection Impact Analysis

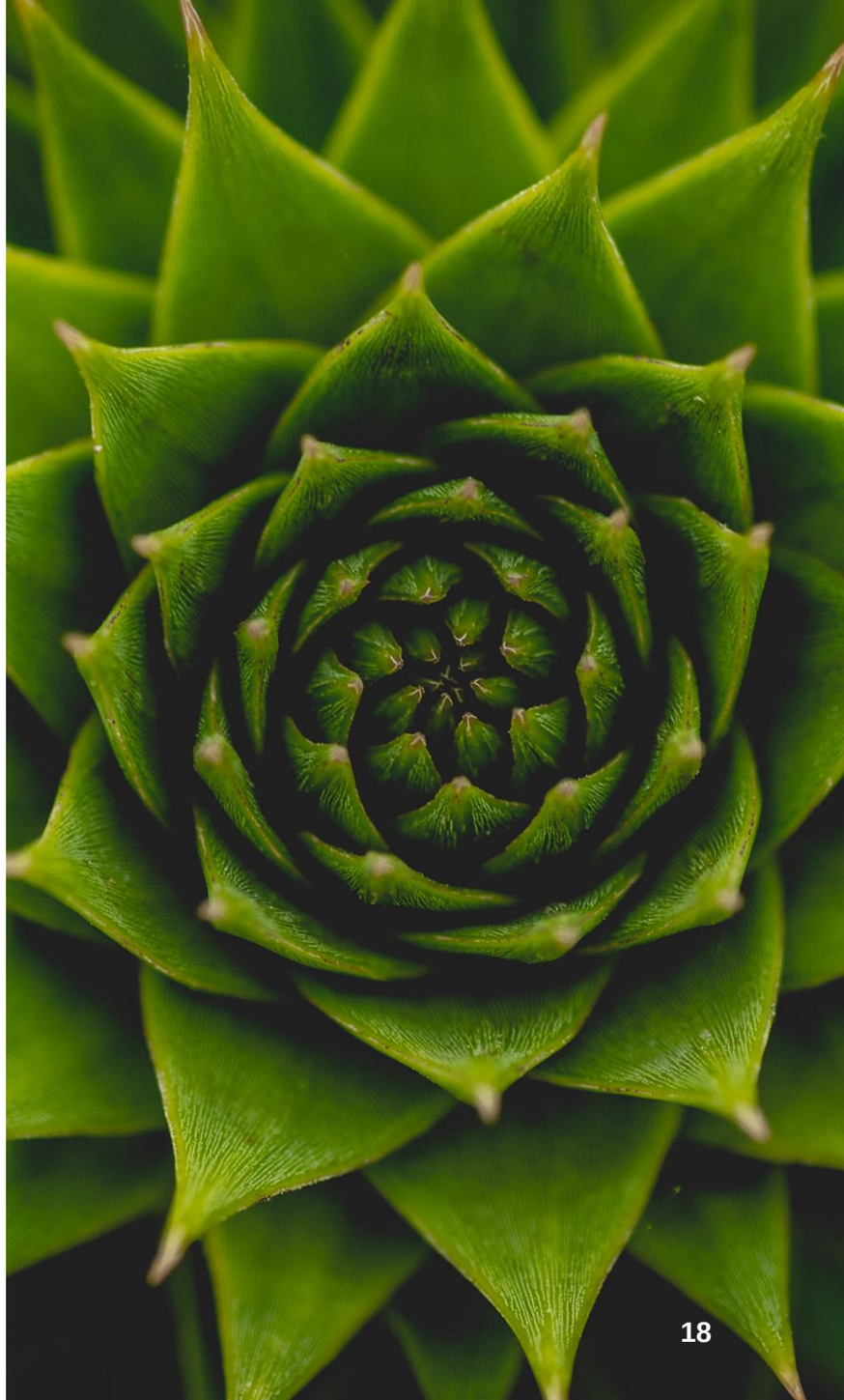
- In case of "**extensive processing**" of health data as special categories of personal data (Art. 35 para 3) a DPIA must be made, also in case of high risk to the rights and freedom of natural persons (assumed in case of gene diagnostics; use of new technologies)
  - Whitelists and blacklists by authorities for guidance
  - “extensive processing” determined on basis of factors such as number of patients, data quantity involved, period of processing and geographical scope (regional, national, international)
- Content:
    - Description of the planned data processing operation
    - Identification of risks
    - Assessment of the risk with regard to possible consequences and damage
    - Auditing the necessity of the data processing operation
    - Description of existing countermeasures and safeguards
    - Verification of the effectiveness of countermeasures and safeguards
    - Final risk assessment, proportionality test
    - Documentation
    - If necessary, consultation with the supervisory authority
    - Implementation of the selected countermeasures and safeguards.
    - Regular review

Specific factors in the legal framework in China

- China has bigger data-sets of medical research, often covering entire provinces; usable data in Western countries often more restricted
  - More data allows to train algorithms to take over functions such as diagnosing diseases from medical images/scans
- Problems in hospital environment reported that hospitals sell patient data without consent
    - (FT, „*China sets the pace in adoption of AI in healthcare technology*“, 31 January 2022)
- Some measures for protection of data may encounter problems under other laws, such as the Cryptography Law
- Foreigners are restricted in relation to access and use of genetic information in China under the Human Genetic Resources Administrative Regulations

Prohibited actions in China for foreigners: Collect, preserve, export, purchase or sell

- Article 7 Administrative Regulations on Human Genetic Resources ("HGR"): "Foreign organizations and individuals, as well as their established or actually controlled institutions**, shall not collect or preserve China's human genetic resources within the territory of China, nor provide China's human genetic resources abroad**."
- It is **prohibited to purchase or sell** human genetic resources. Lawful supply or utilization of human genetic resources for the purpose of scientific research and payment or collection of reasonable costs shall not be deemed a business, Art. 10 HGR.
- Expanded definition of Foreign Parties covers not only foreign-invested enterprises, but also domestic companies actually controlled by foreign shareholders through a VIE structure
- HGR prohibits Foreign Parties from independently sampling or biobanking any China HGR in China, and it adds an approval requirement for the sampling of certain HGR and biobanking of all HGR by Chinese parties.



Need for domestic collaborators

- Article 21 HGR: “Foreign organizations and those institutions established or actually controlled by foreign organizations and individuals which intend to utilize China's human genetic resources to carry out **scientific research activities**, shall comply with Chinese laws, administrative regulations and other pertinent state regulations and, for this purpose, **cooperate with Chinese scientific research institutions, colleges and universities, medical institutions and enterprises**.”
- Art. 22 HGR, International cooperation shall meet the following conditions:

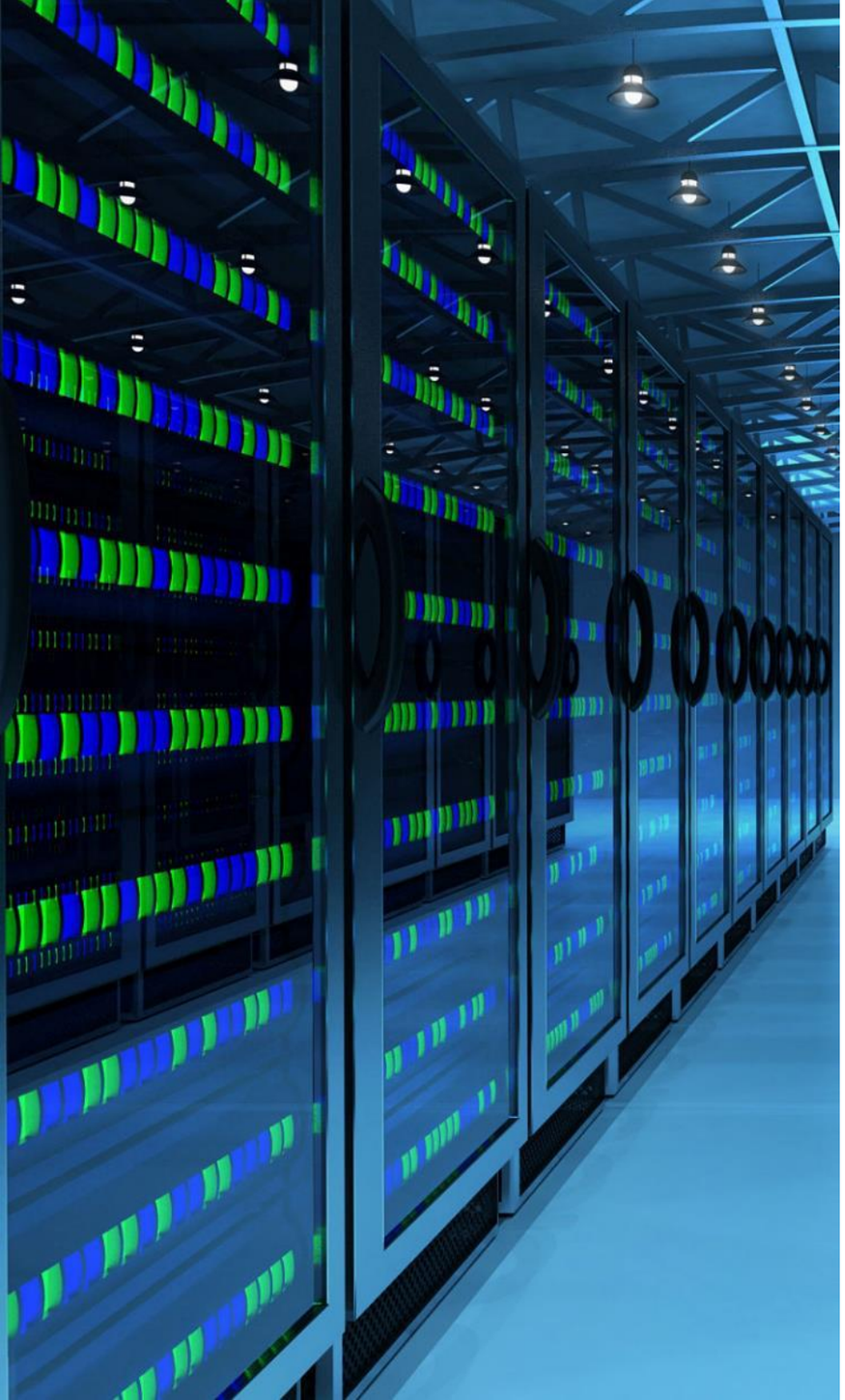
1. not endanger the public health, state security and public interests in China;
2. both parties be a Chinese entity and foreign entity having the qualification of legal person and the basis for and capability of performing relevant work;
3. have specific and lawful goals and contents of cooperative research and a reasonable period;
4. have reasonable cooperative research plans;
5. have lawful sources of the human genetic resources to be utilized, and the categories and quantities corresponding to the research subject;
6. have passed the ethical examination in the country (region) where either party is located; and
7. **have clear agreements on the ownership of research achievements and have a reasonable and specific plan for profit distribution**.

Requirements for international research

- **Change in projects, Art. 23 HGR**: Procedures for examination and approval of changes must be anew completed.
- **Partaking in research by Chinese party**, Art. 24(1) HGR: **It shall be ensured that the Chinese entity and its research personnel can take part in research substantially in the whole process for the duration of cooperation** and the Chinese entity can access and copy all records and data information and other related materials generated from research.
- **Joint patent ownership**, Art. 24(2) HGR: **Joint patent ownership for joint R&D results**. As for other scientific achievements generated from research, the two parties may specify the rights of use and transfer and the methods for interest sharing in the cooperation agreement; in the case of no such agreement, the two parties shall have the right of use; however, transfer to a third person must be subject to the consent of the two parties, and the income therefrom shall be shared by the parties in proportion to their own contributions.
- **Must-have: Agreement**, Art. 25 HGR.
- **Report obligation**, Art. 26 HGR: As for international cooperation in scientific research on the basis of China's human genetic resources, the two parties shall, **within six months after closure of the international cooperation, jointly submit a report** on cooperative research to the administrative department for science and technology under the State Council.

Export from China and security assessment

- Art. 28 HGR if human genetic resources are supplied to or utilized in an open manner by foreign organizations and individuals
  - it shall not endanger the public health, state security and public interests in China;
  - In the case of contingent effect on the public health, state security and public interests in China, it is necessary to pass the **security examination** of MOST (link to Cybersecurity Law?);
  - If the information of human genetic resources is supplied to or utilized in an open manner by foreign organizations and individuals, as well as their established or actually controlled institutions, it is necessary to **submit to the administrative department for science and technology under the State Council for filing the relevant information for backup**;
  - The **two parties may utilize** the information of human genetic resources generated from international cooperation in scientific research on the basis of China's human genetic resources.



4 | Transfer of data

TaylorWessing

Data use by foreign participants in research

Application of GDPR to processing of personal data of data subjects who are in the EU by a controller or processor not established in the Union, where processing activities of personal data are related to offering services or goods to such data subjects or serves the monitoring of their behaviour taking place in the EU:

- Obligation to designate a representative in the EU in case of procession of health data falling under Art. 9 para 1, Art. 27 GDPR
- Unless an exception under Art. 27 para 2 GDRP applies (NOT the case for personal data processing falling under Art. 9 GDPR at a large scale)

Data transfer abroad to third countries, Art. 44 et seq. GDPR

Personal data may only be transferred to a country outside the European Union if

- an adequate level of data protection is guaranteed there, Art. 45 GDPR (in connection with Art. 6,9, 26, 28 GDPR);
- If the EU Commission has not determined the adequacy by means of a corresponding resolution, a transfer may take place if suitable guarantees are provided, see Art. 46 para 2 and 3 GDPR;
  - Companies can create such guarantees for intra-group data flows by means of so-called Binding Corporate Rules (BCR);
  - The parties involved can conclude EU standard contractual clauses (SCC) both within the group and between companies.

“Schrems I” and “Schrems II” decision of ECJ invalidating safe-harbor and privacy shield agreement with US

- In particular the monitoring programs and access authorizations by government take precedence over privacy rights of EU citizens
- The ECJ recognizes that not every encroachment on the fundamental rights of EU citizens results in an infringement. However, the regulations standardized in U.S. law are disproportionate. The requirements for measures by U.S. authorities and their scope are not sufficiently precisely regulated in U.S. law and the interventions are consequently not sufficiently limited. In addition, the surveillance programs do not ensure that surveillance is limited to properly selected target persons. Ultimately, the collection of personal data would not be sufficiently limited. Finally, there is a lack of effective legal protection instruments for EU citizens to take action against measures taken by U.S. authorities - in particular before independent courts - and to enforce rights.

China as comparable case?

- It is not sufficient according to the ECJ to simply contractually agree on Standard Contractual Clauses if there is actually no proportionate protection of the data transferred. If the data exporter fails to conduct the required case-by-case analysis or if the level of data protection is not equivalent, these transfers are potentially invalid.
- Data exporters may establish an adequate level of protection itself, whereby the contractual regulations and the legal system of the country of destination within the meaning of Art. 45 para 2 GDPR are to be taken into account when assessing equivalence.
- This **requires a proportionality assessment in which the level of data protection - in particular state powers of intervention, local data protection supervision and possible legal remedies for EU citizens - must be examined for each destination country and weighed against parameters of the contractually agreed data processing**. In addition to the type of data processed and the scope of the intended processing, these include the protection-enhancing measures. The latter can be of a technical-organizational nature, such as local encryption and/or transport encryption, but also the obligation of the data importer to take (extra-)judicial action against access by authorities or corresponding inquiries.
- The court emphasized that companies must refrain from transferring data to third countries unless there is an adequate level of data protection and there is no mechanism in place beyond the SCC to ensure the required protection in the destination country. Furthermore, the supervisory authorities are obliged to prohibit data transfers if they are not stopped by the companies themselves.
- EU Commission in 2021 has issued new SCC for international data transfer, but unclear whether this eliminates the risk assessment requirement for the individual country and case

Relevant laws and regulations under Chinese law

- No constitutional right to privacy and/or protection of right to one‘s data; see report „Government access to data in third countries“, Final Report EDPS/2019/02-13 of November 2021; Art. 40 Constitution limited in practice
- New regime for personal information protection, e.g. Cybersecurity Law (2017), Personal Information Protection Law and Data Security Law (both 2021)
- Access of government very broad under further laws and regulations
- As such, there is no right of defense against use of personal data also of foreigners by government
  - However, Art 110 (privacy), 111 (personal data) Civil Code, Tort Law, SPC Interpretation grant civil rights to defend privacy, Art. 127 stipulates „Where the law contains provisions in respect of the protection of data and network virtual property, such provisions shall apply.“

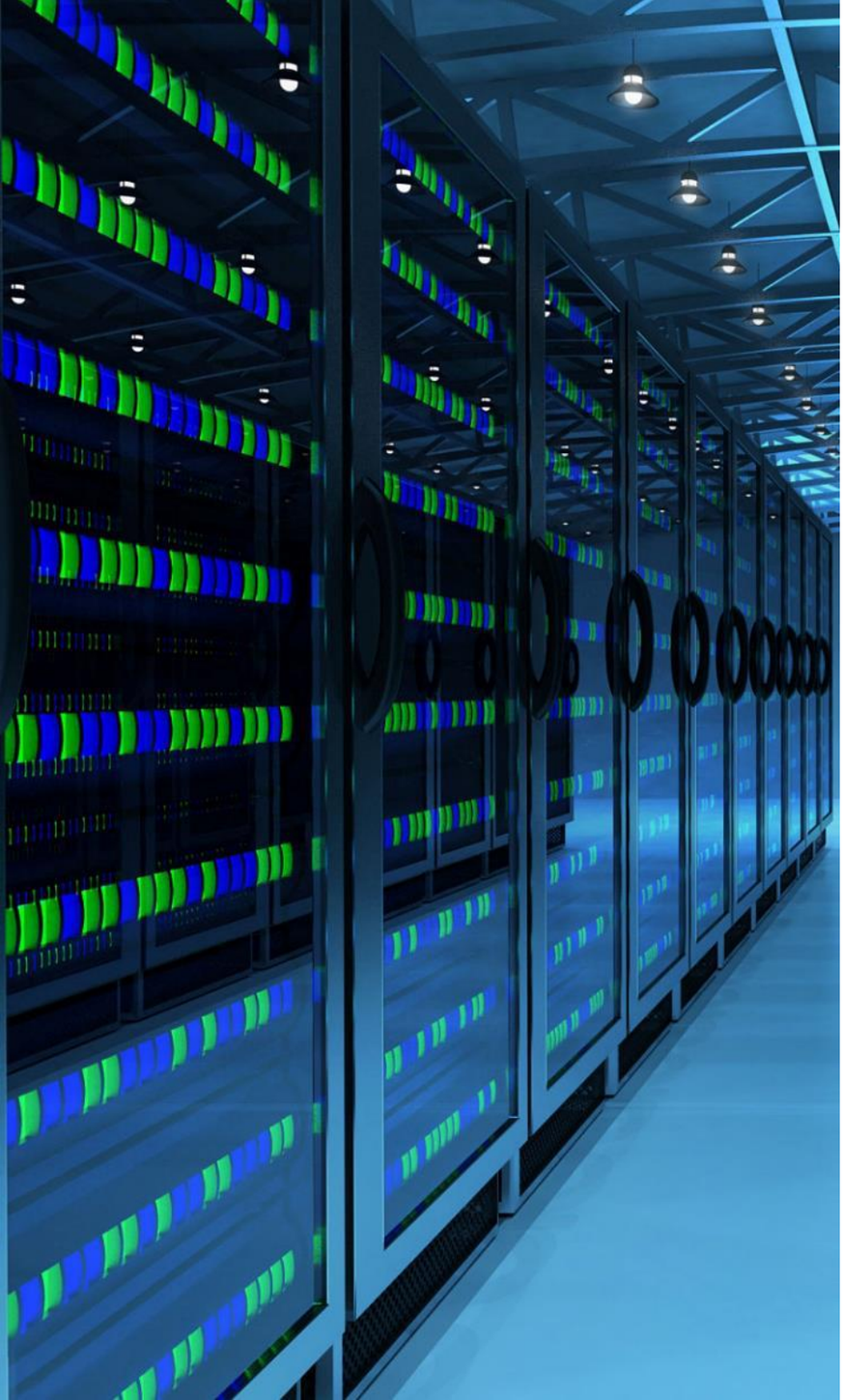
Data transfer – exceptions according to Art. 49 GDPR (a) – (c)

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
   - Risk of ineffectiveness as a result of an incomplete or non-transparent presentation of the possible risks of the third-country transfer
   - Problems in case of any withdrawal of consent

b) the transfer is **necessary** for the performance of a **contract between the data subject and the controller** or the implementation of pre-contractual measures taken at the data subject's request;
   - In the case of a transfer for the performance of a contract with the data subject, an objectively close and substantial connection with the purpose of the contract is required (e.g. travel data for airlines and hotels); necessity may often lack or be unsure

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

Legal dispute and uncertainty whether only actually data exporting party must comply, or also data processor (Art. 4 No. 8, 24 GDPR)



5 | Way forward: Recommendations

TaylorWessing

Checklist for determination of data-related measures to be taken

For determination of respective responsibilities and the data protection relationship of the parties involved, an overview of all data processing operations of the research project must be created. Based on the overview, the responsibility of individual processing activities is determined on the basis of the services owed according to the underlying contracts; subsequently contracts to be created are determined.

Processing activity	e.g. Sponsor	CRO	Auditors	Others (study team etc.)
Creation of consent/legal basis				
Patient treatment				
Selection of data to be reviewed				
Data analysis				
Data storage				
Secondary use of data				

Typical problems

- Use restrictions on genetic resources for certain parties
- Legitimization of research only on consent-basis for sensitive personal information problematic
  - Broad/dynamic consent requirement may have to be defined in law
- Requirements for valid consent must be clarified
- Transfer into third countries currently subject to many legal risks
  - ECJ requirements and how to provide adequate guarantees must be further defined
  - Abstract compliance with data protection requirements instead of individual analysis?
  - Agreement on what technical measures are sufficient for anonymization; increase of pseudonymization where possible on unified standards
  - Increase of transparency of use of personal data by data processors

Recommendations

- (Medical) research too often fails due to legal uncertainty, especially in the area of data protection law. Data sharing between players in the private sector also takes place only to a very limited extent:
  - According to a study conducted by the Institute of German Business on behalf of the BDI, 74% of over 500 companies surveyed consider data sharing with other companies to be "undesirable“, and among the large companies surveyed, the figure is as high as 77%.
  - 85% of the companies surveyed cite gray areas under data protection law and 84% "lack of clarity regarding the rights to use the data" as the main reasons for data not being shared
    - (BDI, Study on the Data Economy in Germany, p. 40) – see citation in Specht-Riemenschneider/Blankertz, MMR 2021, 369
- A case for data escrow services compared to data transfer?
  - Risk of over-regulation
  - Missing global certification standards
- In case of political preference for specific cooperation with certain countries, Art. 45 para 3 GDPR selective implementing act as “way out”

Europe > Middle East > Asia

taylorwessing.com