MASTER THESIS | MASTER'S THESIS

Titel | Title

Balancing Privacy and Innovation: Data Protection and Ethics in EU-China Preclinical Cancer Research Collaborations

verfasst von | submitted by

Judith Christina Loacker-Barth BSc MSc

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 999 083
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von | Supervisor:	Univ.-Prof. Mag. Dr. Nikolaus Forgó

Table of contents

List of abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz (BDSG), BGBl I 2017, No 65. (Federal Data Protection Act)
CAC	Cyberspace Administration of China
CBDF	Cross-Border Data Flow
CBDF Provisions	Provisions on Promoting and Regulating the Cross-Border Flow of Data, issued 22.03.2024, original: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm, English translation: https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/ (accessed 01.02.2026).
CBDT	Cross-Border Data Transfer
CBL	Chinese Biosecurity Law (CBL), issued 18.10.2020, amended 2024, original: http://www.xinhuanet.com/politics/2020-10/18/c_1126624481.htm, English translation: https://www.lawinfochina.com/display.aspx?id=43149&lib=law (accessed 01.02.2026).
CDX	Cell-Derived Xenograft
CFR	Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012
CIIO	Critical Information Infrastructure Operator
CIOMS	Council for International Organizations of Medical Sciences
CIOMS Guidelines	CIOMS, International Ethical Guidelines for Health-related Research Involving Humans, Geneva 2016, https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf (accessed 01.02.2026).
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés (Data Protection Authority France)
CoC	Code of Conduct
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CRO	Contract Research Organization
CSL	Cybersecurity Law of the People's Republic of China (CSL), issued 07.11.2016, original: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm, English translation: https://www.lawinfochina.com/Display.aspx?LookType=1&Lib=law&Cgid=283838&Id=22826&SearchKeyword=&SearchCKeyword=&paycode= (accessed 01.02.2026).
DoH	World Medical Association, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants, issued June 1964, last amended October 2024, https://www.wma.net/policies-post/wma-declaration-of-helsinki/ (accessed 01.02.2026).
DoT	World Medical Association, Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, issued October 2002, last amended October 2016, https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/ (accessed 01.02.2026).
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSL	Data Security Law of the People's Republic of China (DSL), issued 10.06.2021, original: https://www.moa.gov.cn/ztzl/zhnyzxd/zcfg/zybs/flfg/202501/P020250115579606737948.pdf, English translation: http://www.npc.gov.cn/english-npc/c2759/c23934/202112/t20211209_385109.html (accessed 01.02.2026).
ECHR	European Court of Human Rights
EDPB	European Data Protection Board

EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
EHDS	Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, OJ L 2025/327, 05.03.2025.
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCS	ENISA, EUCS – Cloud Services Scheme
EU-SCC	EU Standard Contractual Clauses
FOG	Forschungsorganisationsgesetz BGBl 1981/341 version of BGBl I 52/2023 (Austrian Research Organisation Act)
FTZ	Free Trade Zone
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016
HGR	Human Genetic Resource
HGR Regulation	Regulation of the People's Republic of China on the Administration of Human Genetic Resources (HGR Regulation), issued 28.05.2019, original: https://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm, English translation: https://www.chinalawtranslate.com/en/p-r-c-regulation-on-the-management-of-human-genetic-resources/ (accessed 01.02.2026).
ICH	International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use
IRB	Institutional Review Board
JCA	Joint Controller Agreement
MOST	Ministry of Science and Technology (China)
NHC	National Health Commission (China)
NIH	National Institutes of Health (USA)
NPCSC	National People's Congress Standing Committee (China)
OECD	Organisation for Economic Co-operation and Development
PDX	Patient Derived Xenograft
PHI	Population Health Information (China)
PII	Personally Identifiable Information (China)
PIPIA	Personal Information Protection Impact Assessment (China)
PIPL	Personal Information Protection Law (PIPL), issued 20.08.2021, original: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm, English translation: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (accessed 01.02.2026).
RACI	Responsible, Accountable, Consulted, Informed (role matrix)
REC	Research Ethics Committee
RMB	Renminbi (Chinese currency); Exchange rate RMB 1 = EUR 0,1222; 07.02.2026 European Central Bank.
RNA	Ribonucleic Acid
SA	Supervisory Authority (EU)
SC	Standard Contract for Cross-border Transfer of Personal Information, https://www.glo.com.cn/UpLoadFile/Files/2023/3/1/11535343a7a943e1-f.pdf (accessed 01.02.2026).
SC Measures	Measures on Standard Contracts for the Export of Personal Information (SC Measures), issued 03.02.2023, original: https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm, English translation: https://www.chinalawtranslate.com/en/personal-information-export-contract/ (accessed 01.02.2026).
TIA	Transfer Impact Assessment (EU)

TOMs	Technical and Organizational Measures
UNESCO	United Nations Educational, Scientific and Cultural Organization
WHO	World Health Organization
WMA	World Medical Association

List of figures

1. Introduction

1.1. Background and significance of preclinical research

The World Health Organization (WHO) estimates that nearly 20 million people received a new cancer diagnosis in 2022.[1] In 2022 cancer accounted for 3 in 10 premature deaths caused by noncommunicable diseases among individuals aged 30-69 years and ranked among the top three causes of mortality in this age group in 177 of 183 countries. This disease is one of the most significant challenges for society, public health and the economy in this century.[2] The development of novel therapies to treat cancer requires the international exchange of highly sensitive genetic and health data, as well as human biospecimens.[3]

In an era of rapidly advancing biomedical research and global collaboration, the responsible processing and sharing of genetic and health data have become a key challenge. Preclinical cancer research is essential for developing new therapies and understanding tumor biology. It relies on the systematic collection and analysis of diverse biological materials and associated genetic and health data. Utilizing such data and genetic material is subject to high ethical standards as well as strict data protection regulations.[4] Innovative models such as PDX and organoids illustrate these challenges.[5] While these models are regarded as state-of-the-art tools in oncology research, e.g. to predict therapeutic response, they raise complex questions about the governance of biospecimen and associated data, illustrating the intersection of data protection, ethics and scientific innovation.

International cooperation is particularly critical in oncology, where access to genetically diverse patient populations enables the identification of rare mutations, the validation of biomarkers and the development of targeted therapies.[6] EU-China collaborations, strategically prioritized under Horizon Europe,[7] provide researchers with access to China's large patient

---

[1] *Ferlay at al.*, Global Cancer Observatory: Cancer Today, World, https://gco.iarc.who.int/media/globocan/factsheets/populations/900-world-fact-sheet.pdf (accessed 01.02.2026).

[2] *Bray at al*., Global cancer statistics 2022: GLOBOCAN estimates of incidence and mortality worldwide for 36 cancers in 185 countries, CA Cancer J Clin 2024, 229-230; *Bray et al.*, The Ever-Increasing Importance of Cancer as a Leading Cause of Premature Death Worldwide, Cancer 2021, 3029-3030.

[3] *Wildiers/Adam/O'Reilly/et al.,* Enhancing Clinical Cancer Research Through Sharing of Data and Biospecimens, JAMA Oncology 2025, https://jamanetwork.com/journals/jamaoncology/article-abstract/2843053 (accessed 19.12.2025).

[4] See *Ktr,* Cell Line Establishment Methods: Biomedical Research Advances and Challenges, Stem. Cell. Res. Reg. Med. 2023, 103-105; *Si et al.,* Tumor organoids in immunotherapy: from disease modeling to translational research, Journal for ImmunoTherapy of Cancer 2025, 1-14; National Cancer Institute, National Cancer Institute, Biospecimen Best Practice Introduction, https://dctd.cancer.gov/data-tools-biospecimens/biospecimens-biobanks/resources/best-practices/biospecimen-resources/intro (accessed 31.10.2025); *Siolas/Hannon,* Patient Derived Tumor Xenografts: transforming clinical samples into mouse models, Cancer Research 2013, 5315-5319.

[5] See *Jung,* Human Tumor Xenograft Models for Preclinical Assessment of Anticancer Drug Development, Toxicological Research 2014, 4; *Morton/Houghton,* Establishment of human tumor xenografts in immunodeficient mice, Nature Protocols 2007, 247-250; *Yang et al.,* Tumor organoids for cancer research and personalized medicine, Cancer Biology & Medicine March 2022, 319-332.

[6] *Sirugo/Williams/Tishkoff,* The Missing Diversity in Human Genetic Studies, Cell 2019, 26; Wang et al., Targeting rare tumors: new focus for clinical research in China, EMBO Molecular Medicine 2023, 1-4.

[7] The EU has funded the IMMUNOCAN research collaboration (research partners: Fudan University Shanghai Cancer Center (China) and Institut Mérieux (France)) between 2012 and 2015 to foster medical partnership between China and EU states aimed at the discovery of immune system profiles that potentially act as individualized indicators for cancer (European Commission (CORDIS), Toward enhancing activities of European institutions in the FDUSCC-IM cancer research joint institute in China, https://cordis.europa.eu/article/id/92712-euchina-collaboration-combats-cancer (accessed 31.10.2025)).

base and unique genetic diversity.[8] For example, the EGFR mutation occurs more frequently in Asian patients (in approx. 49 percent of cases), compared to 13 percent in European cohorts. This mutation functions as a biomarker for targeted therapies in non-small cell lung cancer and determines eligibility for highly specific medications. This example demonstrates why access to Asian patient data is crucial in preclinical research. It enables the identification and validation of biomarkers that would otherwise remain undetected in predominantly European datasets.[9]

Even though research collaborations across borders are important for preclinical research, regulatory discrepancies present significant barriers to effective collaborations. China's data protection framework, as well as sector-specific regulation such as the Biosecurity Law and Human Genetic Resources (HGR) Regulations, frames genetic data as a national strategic resource[10], subject to strict export controls and mandatory state approvals. This security-focused approach contrasts with the EU's rights-based model under the GDPR[11], creating ethical and legal tensions in joint research projects.[12] The dynamic evolution of these regulatory regimes adds further complexity, requiring ongoing monitoring and adaptation by researchers and institutions.[13]

International standards, charters and guidelines, such as the Charter of Fundamental Rights of the European Union (CFR), the CIOMS' International Ethical Guidelines for Health-related Research Involving Humans (CIOMS Guidelines), the Declaration of Helsinki (DoH) and Declaration of Taipei (DoT) by the World Medical Association (WMA) provide additional frameworks for ethical data processing in biomedical research. These standards emphasize autonomy,

---

[8] The WHO's Global Cancer Observatory reports on 4,82 million new cancer cases and 2,57 million cancer deaths in China in 2022; *Ferlay et al.,* Global Cancer Observatory: Cancer Today, China, https://gco.iarc.who.int/media/globocan/factsheets/populations/160-china-fact-sheet.pdf (accessed 01.02.2026); *Bray et al.*, CA Cancer J Clin 2024, 229-263.

[9] Medizinische Universität Wien, EGFR-Mutationen reagieren unterschiedlich auf Behandlung, https://www.meduniwien.ac.at/web/ueber-uns/news/detail/egfr-mutationen-reagieren-unterschiedlich-auf-behandlung/ (accessed 19.12.2025); *Melosky et al.*, Worldwide Prevalence of Epidermal Growth Factor Receptor Mutations in Non-Small Cell Lung Cancer: A Meta-Analysis, Molecular Diagnosis & Therapy 2022, 13; *Midha/Dearden/McCormack*, EGFR mutation incidence in non-small-cell lung cancer of adenocarcinoma histology: a systematic review and global map by ethnicity (mutMapII), Am J Cancer Res 2015, 2894.

[10] *McKibbin/Shabani*, Genomic Data as a National Strategic Resource: Implications for the Genomic Commons and International Data Sharing for Biomedical Research and Innovation, *Journal of Law, Medicine & Ethics* 2023, 301-302.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016.

[12] *Li/Cong/Liu*, Research under China's personal information law, Science 2022, 713-715.

[13] For example, the European Commission has issued a proposal for the Biotech Act on 16. December 2025 (See European Commission, Press Release: New measures to make EU health sector more innovative, competitive and resilient, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_3077 (accessed 19.12.2025)).

transparency and fairness and are widely adopted in both EU and international research contexts.[14] They provide a foundation for evaluating the ethical and legal dimensions of cross-border research collaborations, particularly related to consent and the protection of vulnerable populations.

This thesis explores how privacy and innovation can be balanced in EU-China preclinical cancer research collaborations, focusing on the regulatory frameworks and practical challenges involved. While the focus is on preclinical research in oncology, the findings have broader relevance for other areas of biomedical research, offering insights that extend beyond oncology and preclinical research to broader questions of global research governance and compliance strategies.

By analyzing the intersection of data protection, ethics and innovation through the lens of EU-China collaboration, the thesis aims to contribute to operational guidance for researchers and institutions. It further offers a detailed use case to illustrate real-world data flows, regulatory hurdles and compliance solutions, adding to academic and practical understanding of EU-China research collaborations and the utilization of genetic data and material for innovation.

1.2. Research questions, objectives and methodology

1.2.1. Research objectives

The central objective of this thesis is to analyse and compare the legal and ethical frameworks governing the processing and cross-border sharing of genetic data, health data and human biospecimens between parties located in the European Union and Mainland China. Additionally, the thesis identifies practical challenges arising in research collaborations and develops compliance strategies to address them, illustrated through a practical use case.

More specifically, the thesis has the following goals:

(i) To examine the legal provisions under the EU's GDPR and China's data protection and sector-specific laws (Personal Information Protection Law, Data Security Law, Cybersecurity Law, Biosecurity Law and Human Genetic Resource Regulation) that regulate the use and international transfer of sensitive/special category data, namely genetic and health data and human biospecimens.

[14] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012; CIOMS, International Ethical Guidelines for Health-related Research Involving Humans, Geneva 2016, https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf (accessed 01.02.2026); World Medical Association, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants, issued in June 1964, last amended October 2024, https://www.wma.net/policies-post/wma-declaration-of-helsinki/ (accessed 01.02.2026); World Medical Association, Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, issued in October 2002, last amended October 2016, https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/ (accessed 01.02.2026).

(ii) To assess how ethical principles – particularly informed consent and the protection of vulnerable populations – are implemented and interact with legal requirements in cross-border research.

(iii) To identify practical compliance challenges faced by researchers and institutions operating across jurisdictions and to highlight possible compliance strategies.

1.2.2. Research questions

The thesis addresses one primary research question and three secondary questions. In this thesis, "research collaboration(s)" refers specifically to preclinical cancer research collaborations involving health data, genetic data and/or human biospecimen.

The primary research question is:

How do the EU's GDPR and China's data protection laws (PIPL, DSL, CSL) and sector-specific regulatory frameworks (Biosecurity Law, HGR Regulations) regulate the utilization and sharing of genetic data and human biospecimens in cross-border preclinical cancer research between parties located in the EU and China?

The focus is on cancer research, as this field typically utilizes genetic data and human genetic material such as tumor specimens.

The primary research question is supplemented by three additional research questions:

1) What are the key differences and overlaps between the EU's GDPR and Mainland China's data protection regime and sector-specific regulations regarding cross-border data transfers and how do these differences impact research?
2) How can ethical principles, specifically informed consent and the protection of vulnerable populations, be operationalized in EU-China preclinical cancer research collaborations?
3) What practical challenges do researchers face in complying with the GDPR and Chinese regulations and how can those be addressed in operational practice?

1.2.3. Methodology and thesis structure

The core methodology of this thesis is a comparative legal analysis of the European Union and Chinese frameworks governing the data protection aspects of the collection and handling of genetic material and data, with a particular focus on preclinical cancer research collaborations. This includes a detailed examination of the relevant aspects of the European Union's General Data Protection Regulation (GDPR) (especially Article 3, 9, 44–49 and 89 GDPR)[15], the Chinese

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016.

Personal Information Protection Law (PIPL)[16], Data Security Law (DSL)[17], Cybersecurity Law (CSL)[18] and sector-specific legal instruments such as the Chinese Biosecurity Law (CBL)[19] and the Human Genetic Resource Regulation (HGR-Regulation)[20]. In addition, the analysis covers several supplementary guidance documents and international standards governing data transfer aspects, HGR specifications and international ethical guidelines. Methodically, the thesis follows a triangular approach, that combines a descriptive presentation of the relevant norms, a systematic normative comparison, as well as a risk-based assessment of their practical implications.

This thesis focuses on a doctrinal and comparative approach. It first describes the relevant regulations and soft law in the EU and China. The comparison then shows where the two systems align and where they diverge in practice. The evaluative comments and practical assessments are clearly separated from the descriptive parts in Chapter 6 and Chapter 7 and reflect the author's own interpretation.

The analysis focuses primarily on (i) the legal grounds for processing genetic data and human biospecimen, (ii) consent requirements and transparency obligations, (iii) cross-border data transfer mechanisms from the EU to China and vice versa and collaboration requirements, (iv) enforcement mechanisms and (v) data localization and sovereignty-related constraints. The legal comparison aims to identify areas of convergence and divergence, with particular attention to how these differences impact international research collaborations. In parallel, this thesis assesses ethical standards in biomedical research. This includes evaluating informed consent models, the protection of vulnerable populations and the roles of ethics committees. Practical challenges for scientific research and potential compliance strategies are additionally critically analyzed.

At the same time, this thesis aims to take a critical view towards the current fragmentation of legal and ethical frameworks governing EU/China research collaborations. Both jurisdictions pursue legitimate objectives, such as data protection, national security and scientific integrity.

---

[16] Personal Information Protection Law (PIPL), issued 20.08.2021, original: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm, English translation: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (accessed 01.02.2026).

[17] Data Security Law of the People's Republic of China (DSL), issued 10.06.2021, original: https://www.moa.gov.cn/ztzl/zhnyzxd/zcfg/zybs/flfg/202501/P020250115579606737948.pdf, English translation: http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html (accessed 01.02.2026).

[18] Cybersecurity Law of the People's Republic of China (CSL), issued 07.11.2016, original: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm, English translation: https://www.lawinfochina.com/Display.aspx?LookType=1&Lib=law&Cgid=283838&Id=22826&SearchKeyword=&SearchCKeyword=&paycode= (accessed 01.02.2026).

[19] Chinese Biosecurity Law (CBL), issued 18.10.2020, amended 2024, original: http://www.xinhuanet.com/politics/2020-10/18/c_1126624481.htm, English translation: https://www.lawinfochina.com/display.aspx?id=43149&lib=law (accessed 01.02.2026).

[20] Regulation of the People's Republic of China on the Administration of Human Genetic Resources (HGR Regulation), issued 28.05.2019, original: https://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm, English translation: https://www.chinalawtranslate.com/en/p-r-c-regulation-on-the-management-of-human-genetic-resources/ (accessed 01.02.2026).

However, the cumulative effect of divergent consent models, cross-border data transfer restrictions and localization leads to disproportionate practical barriers for collaboration. These barriers manifest in long approval timelines, multiple compliance processes and legal uncertainties that potentially discourage parties from engaging in joint projects.

The research draws on primary legal texts, regulatory guidelines, academic literature and policy reports. Chinese sources are used in English translation. Where no publicly available English translation exists, a translation of the cited Chinese source is provided in Appendix 3. Due to limited judicial interpretation and a dynamic regulatory environment, supplementary Q&A documents and guidance from Chinese authorities were also considered as soft-law sources.

Limitations include the restricted availability of judicial interpretations in China, potential translation ambiguities and the dynamic regulatory environment particularly in relation to cross-border data transfer mechanisms and aspects related to HGR. Chinese national bodies, such as the Cyberspace Administration of China (CAC) and the National Health Commission (NHC) frequently issues new interpretive or guiding documents (e.g. Q&A on Data Outbound Security Management Policy[21] or Q&A on Issues Related to the Management of Human Genetic Resources (Part V)[22], issued in October 2025). Due to lengthy peer-review processes for academic literature aimed at ensuring academic standards are upheld, such new guidance documents are often not yet interpreted in academic literature. Their reflection is limited to non-academic sources such as law firm updates. Lastly, the heterogeneous implementation of relevant norms within the EU remains a practical challenge, however this thesis focuses on legislation at EU level, not considering Member State laws and deviations from core principles in detail. The thesis only addresses selected ethical considerations related to data privacy and does not cover other important ethical considerations, such as animal welfare.

The thesis is structured as follows: Chapter 2 outlines practical data processing in preclinical cancer research and research collaborations, Chapter 3 examines the relevant legal frameworks, Chapter 4 addresses cross-border data transfer mechanisms, Chapter 5 discusses ethical considerations, Chapter 6 highlights practical challenges and corresponding compliance strategies and Chapter 7 presents the conclusion.

[21] Q&A on Data Outbound Security Management Policy, issued 31.10.2025, original: https://www.cac.gov.cn/2025-10/31/c_1763633376984070.htm (accessed 01.02.2026), English translation available in Appendix 3.
[22] Q&A on Issues Related to the Management of Human Genetic Resources (Part V), issued 11.10.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202510/f04ebf5bc27a47e5a1ac6f370b3c5ec3.shtml (accessed 01.02.2026), English translation available in Appendix 3.

Additional materials, such as a tabular comparison of core aspects of Chinese and EU law, a Transfer Impact Assessment for the use case established in Chapter 6 and translations of Chinese sources are provided in the appendices.

2. Data processing in preclinical cancer research and research collaborations

This chapter briefly outlines the practical aspects of data processing in preclinical cancer research collaborations, focusing on biospecimen types, data categories and workflow stages. It further describes the use of xenograft models and organoids to highlight how biospecimens and data are utilized in preclinical research in practice.

Commonly used human biospecimens in preclinical cancer research include tumor tissue, blood samples and cellular derivatives, which are used to generate genomic, transcriptomic and phenotypic datasets. These are essential for understanding tumor biology and evaluating therapeutic efficacy.[23] The data processed in this context include genetic sequences (e.g. DNA/RNA sequences, expression profiles), phenotypic profiles and clinical metadata, such as demographic data, imaging results and treatment outcomes. All of these data categories fall under the GDPR's definition of special categories of personal data and corresponding provisions in Chinese law.[24]

A typical data lifecycle in preclinical cancer research collaboration involves several stages. First, the biospecimens and associated data are collected from patients and in some cases from healthy donors who may serve as control (e.g. blood samples). The biospecimens and data are typically sourced from clinical procedures such as biopsies and autopsies[25] and processed for their initial purpose, such as medical treatment and are potentially pseudonymized at this stage. They are stored in biobanks, which act as repositories for long-term preservation and reuse. Biobanks not only facilitate access to biological material but also manage associated personal data, including health data and genetic information.[26] Data and samples undergo quality checks to ensure scientific validity and compliance and are then analyzed locally and, where permitted, collaboratively, using multi-omics[27] and computational methods. They may also be shared with research partners, including across borders, subject to legal and ethical safeguards. In the next step, samples and data may be reused for answering new research questions or destroyed if no longer needed.[28]

---

[23] See *Ktr*, Cell Line Establishment Methods: Biomedical Research Advances and Challenges, Stem. Cell. Res. Reg. Med. 2023, 103-105; *Siolas/Hannon*, Cancer Research 2013, 5315-5319; *Si et al.*, Journal for ImmunoTherapy of Cancer 2025, 1-14; National Cancer Institute, National Cancer Institute, Biospecimen Best Practice Introduction, https://dctd.cancer.gov/data-tools-biospecimens/biospecimens-biobanks/resources/best-practices/biospecimen-resources/intro (accessed 31.10.2025).
[24] Article 9 GDPR; *Morton/Houghton*, Nature Protocols 2007, 247-250; *Yang et al.*, Cancer Biology & Medicine March 2022, 319-332.
[25] *Morton/Houghton*, Nature Protocols 2007, 247.
[26] *Annaratone et al.*, Basic principles of biobanking: from biological samples to precision medicine for patients, Virchows Archiv 2021, 234-236.
[27] Multi-omics is the biological analysis of data of various "omes", e.g. genome, transcriptome and proteome (*Bersanelli et al.*, Methods for the integration of multi omics data: mathematical aspects, BMC Bioinformatics 2016, 168).
[28] *Annaratone et al.*, Virchows Archiv 2021, 234-235; *Staunton et al.*, Frontiers in Genetics 2022, 91-92.

Two advanced model systems, human xenograft models[29] and organoids[30], play a central role in preclinical cancer research. Xenograft models involve implanting human tumor tissue into immunodeficient mice, preserving the genetic characteristics of the original tumor. This allows researchers to explore metastatic behavior and responses to therapeutic treatments in vivo.[31] There are two main types of xenograft models: Cell Line-Derived Xenograft (CDX) models are generated from established human cancer cell lines, maintained and cultured in vitro and implanted into rodents.[32] Patient-Derived Xenograft (PDX) models are generated by transplanting tumor material from primary cancer patients, collected from autopsy and biopsy, directly into mice. This allows researchers to study novel treatments and establish therapies personalized for the individual patient.[33]

Organoids, by contrast, are three-dimensional cultures derived from patient cells that mimic how human tissue is structured and behaves. Both xenografts and organoids enable researchers to study tumor behavior, drug response and resistance mechanisms in controlled settings.[34] As noted, CDX-models and organoids are created utilizing human cell lines. The process of cell line establishment is complex, involving extracting and growing cells from sources like organs, embryos or tissue.[35] Immortalized cell lines used in CDX models and organoids are typically sourced from commercial repositories.[36]

---

[29] See *Khandelwal et al.,* Next-Generation Sequencing Analysis and Algorithms for PDX and CDX Models, Molecular Cancer Research 2017, 1012-1016; *Morton/Houghton*, Nature Protocols 2007, 247-250.
[30] See *Si et al.,* Journal for ImmunoTherapy of Cancer 2025, 1-14; *Yang et al.,* Cancer Biology & Medicine March 2022, 319-332.
[31] See *Morton/Houghton,* Nature Protocols 2007, 247-250; *Khandelwal et al.,* Molecular Cancer Research 2017, 1012-1016.
[32] *Das/Das,* Orthotopic PDX and CDX Mice Model for Cancer Stem Cell Research, in: *Pathak/Banerjee/Bisgin (eds.),* Handbook of Animal Models and its Uses in Cancer Research (2023) 503-504.
[33] *Jung,* Toxicological Research 2014, 4; *Morton/Houghton*, Nature Protocols 2007, 247-250.
[34] See *Yang et al.,* Cancer Biology & Medicine March 2022, 319-332.
[35] *Ktr,* Cell Line Establishment Methods: Biomedical Research Advances and Challenges, Stem Cell Research and Regenerative Medicine 2023, 103-105.
[36] The most prominent ones are the American Type Culture Collection (ATCC)(USA), the Leibniz-Institute DSMZ and the European Collection of Authenticated Cell Cultures (ECACC) (See *Mirabelli/Coppola/Salvatore,* Cancer Cell Lines Are Useful Model Systems for Medical Research, Cancers 2019, 9); One of the most prominent cell lines are the HeLa Cell Lines, stabilized in 1953 from a cancer patient named Henrietta Lacks. The derivation of the HeLa cells makes a significant milestone in cell biology. The cells played an important role in enabling the development of the polio vaccine and have been cited in more than 16.000 publications in cancer research (See *Mirabelli/Coppola/Salvatore,* Cancers 2019, 2-4).

3. Legal frameworks for data protection in the EU and China

3.1. Overview of key data protection laws and sector-specific regulations

The landscape of data protection legislation in the context of preclinical cancer research collaborations between researchers in the European Union and in China is shaped by a complex interplay of general data protection laws complemented by sector-specific regulations. Understanding this regulatory environment is essential for researchers and institutions navigating cross-border projects that involve genetic data and human biospecimen.

At the core of the European Union's data protection regulation is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).[37] The GDPR establishes comprehensive rules for the processing of personal data, including the processing of special categories of personal data such as genetic and health information. The GDPR is renowned for its extraterritorial reach, robust data subject rights and stringent requirements for transparency, consent and security. In the context of scientific research, the regulation provides specific derogations and safeguards designed to balance personal data protection while advancing innovation and research.[38] In the EU, biobanking and the use of human biospecimens, such as in PDX-models, are subject to national laws and ethical guidelines that complement the GDPR.[39] Since a detailed examination of EU-Member State laws would be beyond the scope of this thesis, the thesis focuses on Union law and international ethical guidelines.

China's regulatory framework, in contrast, is characterized by a combination of general data protection statutes with targeted sectoral rules. Together, the PIPL, Data Security Law (DSL)[40] and Cybersecurity Law (CSL)[41] form China's overarching regulatory framework for collecting, processing and transferring personal information, which particularly emphasize national security and data sovereignty.[42] These laws are supplemented by sector-specific instruments such as the Human Genetic Resources (HGR) Regulations[43] and the Chinese Biosecurity Law

[37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016.
[38] See especially Article 3, 4, 9, 44-49 and 89 GDPR.
[39] *Staunton et al.*, Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research, frontiers in Genetics 2022, 1-2.
[40] Data Security Law (DSL), effective 2021.
[41] Cybersecurity Law (CSL), effective 2017.
[42] See *McKibbin/Shabani*, Journal of Law, Medicine & Ethics 2023, 301-313.
[43] Regulation of the People's Republic of China on the Administration of Human Genetic Resources (HGR Regulation), issued 28.05.2019, original: https://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm, English translation: https://www.chinalawtranslate.com/en/p-r-c-regulation-on-the-management-of-human-genetic-resources/ (accessed 01.02.2026).

(CBL)[44], which impose additional requirements on handling, export and ethical oversight of genetic material and associated data.

This chapter provides an overview of the key legal instruments governing data protection and sector-specific regulations in the EU and China. It sets forth the foundation for the subsequent analysis of how these frameworks impact preclinical cancer research collaborations, with particular attention to the challenges and compliance strategies in cross-border projects.

Since one of the core aspects of cross-border research collaborations is the transfer of personal data and obligations related to data localization and collaboration, those topics are discussed separately and in detail in Chapter 4.

3.2. European Union: GDPR and research data

The European Union's General Data Protection Regulation (GDPR) provides a comprehensive regulatory framework governing the processing of personal data, setting out the conditions under which the Regulation applies to controllers and processors in and outside the European Union.[45]

Article 3 GDPR determines the territorial scope of the legislation, marking a significant expansion of the applicability compared to previous EU data protection legislation. The establishment criterion as defined in Article 3(1) GDPR ensures that any personal data processing carried out by entities established in the EU is governed by the GDPR. This is independently as to where the processing of personal data is taking place and as to whether the entity processing the data is the controller or processor.[46] Processing personal data "*in the context of the activities*" of an EU establishment is sufficient for GDPR to apply.[47] The second criterion determining the need for GDPR compliance is the targeting criterion.[48] It extends the applicability of GDPR to non-EU controllers and processors that either target individuals in the Union by offering goods or services on the Union's market or that track the behavior of persons within the EU.[49]

The processing of genetic data and human biospecimen falls therefore within the scope of GDPR, when it occurs in the context of the activities of a data controller established in the Union, even if the processing is carried out by a processor or joint controller located in China, provided that there is a demonstrable link to the EU-based operations of the data controller.[50]

---

[44] Chinese Biosecurity Law (CBL), issued 18.10.2020, amended 2024, original: http://www.xinhuanet.com/politics/2020-10/18/c_1126624481.htm, English translation: https://www.lawinfochina.com/display.aspx?id=43149&lib=law (accessed 01.02.2026).
[45] Article 3 GDPR.
[46] EDPB, Guidelines 03/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, adopted on 12.11.2019, 4-5.
[47] EDPB, Guidelines 3/2018, 2019, 9.
[48] Article 3(2) GDPR.
[49] EDPB, Guidelines 3/2018, 2019, 13.
[50] Recital 22 GDPR.

The GDPR provisions apply to every stage of the genetic research lifecycle. From the initial collection of human specimens and related personal data, through the storage and preparation to the utilization of the data and material for secondary research purposes and the destruction or depletion of biospecimens.[51] Genetic data is explicitly defined in GDPR as "special category of personal data", information which is highly sensitive in nature due to its potential for misuse.[52] Additionally, it contains not only information about the specific person the genetic data were derived from, but potentially also about their family members.[53] Genetic data is defined in GDPR as personal information reflecting an individual's inherited or obtained genetic traits and provides distinctive insights into this person's health status and physiology. It is classically derived from the examination of biological materials – such as DNA (chromosomal, deoxyribonucleic acid), RNA (ribonucleic acid) or other molecular components – that reveal genetic characteristics unique to the individual.[54]

Biological specimens per se do not constitute personal data under GDPR, however the act of deriving data from the genetic material corresponds to the collection of genetic information.[55]

Processing of special-category data is prohibited unless a ground in Article 9(2) GDPR applies, notably explicit consent (Article 9(2)(a) GDPR), substantial public interest (Article 9(2)(g) GDPR), public interest in the area of public health (Article 9(2)(i) GDPR) and scientific research (Article 9(2)(j) GDPR) in conjunction with Article 89 GDPR. Processing special categories of personal data based on Article 9(2)(g), (i) or (j) GDPR must be laid down in Union or Member State law with safeguards. The Member States can further impose supplementary rules or constraints for the processing of biometric, genetic or health data.[56] European case law[57] suggests that the concepts of necessity and public interest are interpreted as requiring a "*pressing social need",* rather than serving predominantly private or commercial interests.[58]

3.2.1. Consent and transparency

Human biospecimens and genetic data are frequently obtained by healthcare institutions and subsequently stored in biobanks. This typically occurs in the context of clinical trials, routine

[51] *Hallinan*, Broad consent under the GDPR: an optimistic perspective on a bright future, Life Sciences, Society and Policy, 2020, 1.
[52] Article 9 GDPR.
[53] *Shabani/Borry*, Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation, European Journal of Human Genetics 2018, 149.
[54] Article 4 (13) GDPR, Recital 34 GDPR.
[55] *Faymann et al.,* Digital health innovations — Good practice guide for obtaining consent for the use of personal health information for re-search and innovations, https://www.cencenelec.eu/media/CEN-CENELEC/News/Workshops/2023/2023-03-15%20-%20Digital%20Health/draftcwa.pdf (accessed 01.02.2026), 30.
[56] Article 9(4) GDPR.
[57] See ECHR 07.12.1976, 5493/72, Handyside v. the UK; ECHR 26.03.1987, 9248/81, Leander v. Sweden.
[58] EDPS, A Preliminary Opinion on data protection and scientific research, published 06.01.2020, https://www.edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf (accessed 01.02.2026), 23.

medical treatment or through targeted donations specifically intended for biobanking and research purposes.[59] Due to their sensitive nature, GDPR typically requires explicit consent from data subjects for the processing of their genetic data. Consent must meet certain requirements, as stated in Article 4(11) GDPR, to be valid, namely it must be specific, freely given, informed and unambiguous. [60] In this sense "specific" refers to a sufficiently clear and limited scope of processing. "Freely given" refers to the absence of any form of force, and "informed" means that sufficient information have to be communicated to the data subject enabling them to understand the circumstances and consequences of the processing. Lastly, "unambiguous" refers to a clear intention to consent, expressed through a definitive act of agreement.[61]

Data controllers are required to provide transparent information about the scope and nature of data processing, including the types of personal data involved, the methodology of processing and any third parties with whom the data might be shared.[62] However, in the context of scientific research, particularly in preclinical research, it is often difficult to anticipate all future use cases at the time of data collection and extraction of samples.

The legislator acknowledged this challenge and introduced the concept of broad consent in Recital 33 GDPR. Broad consent allows data subjects to consent to the processing of their data for certain areas or phases of scientific research, rather than for a narrowly defined project. The controller does not need to fully specify all future processing purposes. However, the flexibility is limited. Broad consent is only permissible where it is objectively impossible to define and specify all purposes at the outset. And even then, the research domain must be described as precisely as possible.[63]

Importantly, Recital 33 is not a standalone legal basis. It merely interprets the consent requirements under Article 6 and Article 9 GDPR and does not exempt controllers from meeting the conditions set out in Article 4(11), namely that consent must be specific, informed, freely given and unambiguous.[64] *Herbst* (2016) however, raises the question whether broad consent can even meet the requirement of being informed.[65]

---

[59] *Herbst*, Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, Datenschutz und Datensicherheit 2016, 371.
[60] Recital 32 GDPR.
[61] *Hallinan*, Life Sciences, Society and Policy, 2020, 5.
[62] Article 13 and 14 GDPR.
[63] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 04.05.2020, 30-31, para. 155-156 and 159.
[64] See EDPB, Guidelines 05/2020, 2020, 30-31, para. 156.
[65] *Herbst*, Datenschutz und Datensicherheit 2016, 373.

When relying on broad consent, controllers should implement robust safeguards to mitigate risks associated with a less specific consent. Measures such as pseudonymization, data minimization, and, where technically feasible, anonymization are recommended.[66] The EDPB further highlights that (broad) consent can be withdrawn at any time, while also recognizing that this might erode specific kinds of research where data has to be linked to a person.[67] Furthermore, the reasonable expectations of data subjects impose constraints on the secondary use of genetic data for research purposes.[68]

For scenarios where the processing purpose cannot initially be determined, the EDPB suggests an iterative approach in the form of a "dynamic consent" as a recommended best practice.[69] This model allows data subjects to consent to the purposes in a general manner and for specific steps of a research project that are already defined at the beginning. Before each new project stage, the data subject shall be asked to consent for the following step.[70] Advocates of this consent model highlight benefits such as improving transparency, communication and recruitment, especially when utilizing technology for automatically selecting and approaching data subjects. Dynamic consent further allows withdrawal from individual processing steps and purposes, instead of the usual "all-or-nothing" approach when it comes to consent and its withdrawal.[71]

Ethical implications of consent and practical challenges are discussed in detail in Chapter 5 and 6.

3.2.2. Research exceptions and safeguards

The GDPR seeks to balance privacy with scientific progress by introducing a derogation for scientific research related data processing in Article 89, provided that appropriate safeguards for the rights and freedoms of the data subject are in place.[72]

This "research exception" must be stipulated in Union law or Member State law and might allow derogations from certain data subject rights. Namely the right of access[73], the right to rectification[74], the right to restriction of processing[75] and the right to object[76]. Additionally, the member states have the authority to introduce additional provisions, including restrictions,

[66] EDPB, Guidelines 05/2020, para. 157, 160 and 161.
[67] EDPB, Guidelines 05/2020, para. 163; see also: CIOMS, International Ethical Guidelines for Health-related Research Involving Humans, 2016, Guideline 9.
[68] Recital 47, Recital 50 GDPR.
[69] EDPB, Guidelines 05/2020, para. 159.
[70] *Kaye et al.*, Dynamic consent: a patient interface for twenty-first century research networks, European journal of human genetics 2015, 143-144.
[71] Ibid, 144-145.
[72] *Staunton et al.*, frontiers in Genetics 2022, 1-2.
[73] Article 15 GDPR.
[74] Article 16 GDPR.
[75] Article 18 GDPR.
[76] Article 21 GDPR.

particularly concerning the utilization of genetic, biometric or health data.[77] The legal basis stipulated in EU or Member State law must additionally meet certain requirements, such as (i) being appropriate in relation to the purposes pursued, (ii) preserving the fundamental nature of the right to data protection and (iii) include obligations on appropriate safeguards protecting the rights and freedoms of affected individuals.[78] The latter must include Technical and Organizational Measures (TOMs), particularly targeting data minimization, pseudonymization or anonymization whenever feasible.[79]

To date, several Member States have implemented Article 89(1) GDPR governing safeguards for scientific research related data processing, such as the Austrian Research Organization Act (Forschungsorganisationsgesetz; FOG)[80] or § 27(1) BDSG in Germany[81]. The GDPR itself does not define what constitutes appropriate safeguards, however, additional studies conducted by the EDPB[82] and by researchers[83] provide various suggestions.

The 2019 EDPB study analyzing twelve Member State legislations, guidelines, Code of Conduct and soft law, concludes that first and foremost requirements on pseudonymization and anonymization shall be put in place. The study further highlights measures relating to access control and logging, encryption, confidentiality obligations imposed on staff and appropriate training requirements. All of the measures should be regularly monitored. Further (mandatory) measures are the involvement of independent ethics reviews, appointing a Data Protection Officer (DPO) and conducting a Data Protection Impact Assessment (DPIA).[84]

3.2.3. Pseudonymization and anonymization

The key concept of the European data protection regulation is that of "personal data" which determines the material scope of GDPR as described in Article 2(1) GDPR. In GDPR "personal data" is defined in Article 4(1) as "*any information relating to an identified or identifiable natural person ('data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".[85]

---

[77] Article 9(4) GDPR.
[78] Recital 52 and 53 GDPR; *Duguet/Herveg*, Safeguards and Derogations Relating to Processing for Scientific Purposes: Article 98 Analysis for Biobank Research, in: *Slokenberga/Tzortzatou/Reichel* (eds.), GDPR and Biobanking, Law, Governance and Technology (2021) 108.
[79] Article 89(1) GDPR; Recital 156 GDPR; *Staunton et al.*, frontiers in Genetics 2022, 1.
[80] Forschungsorganisationsgesetz BGBl 1981/341 version of BGBl I 52/2023.
[81] Bundesdatenschutzgesetz (BDSG), BGBl I 2017, No 65.
[82] See EDPB, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, Final Report, published 07.09.2021.
[83] See *Staunton et al.*, frontiers in Genetics 2022, 1.
[84] EDPB, Study on the appropriate safeguards required under Article 89(1) of the GDPR for the processing of personal data for the scientific research, 2019, 64.
[85] Article 4(1) GDPR.

While the processing of personal data is subject to GDPR, the processing of anonymous data is not. Data are considered anonymous when they are stripped entirely of any information, which would allow the identification of the data subject.[86]

The GDPR has further introduced the concept of pseudonymous data in Article 4(5) GDPR, referring to the processing of personal data in a way in which it can no longer be directly linked to an individual without utilizing additional information, such as a code or a key, provided that the additional information is handled separately and in a secure manner.[87] Processing data in a pseudonymous manner is subject to GDPR. Pseudonymous data are commonly regarded as a safeguard under GDPR, as it reduces the risk of identification of the individual by linking the data to the specific person difficult. At the same time, it allows the controller to analyze and, whenever necessary, to connect multiple data sets containing information on the same individual. As pseudonymous data can still be used to re-identify an individual using additional information, even if this information is stored separately, it is considered personal data, subject to GDPR, unless anonymity conditions are met.[88]

While using data in an anonymous or pseudonymous manner is highly encouraged[89], achieving anonymization of genetic data is challenging in practice due to its uniqueness by nature, as well as its potential for re-identification.

Marnau, Berrang and Humbert (2018) argue that while the effective anonymization of genetic data is challenging due to its unique nature, it is not entirely impossible. The authors emphasize that the feasibility of anonymization should be assessed on a case-by-case basis, taking into account the specific context and available safeguards.[90] *Herbst* (2016) notes that anonymization in biobanking contexts can potentially be achieved by deleting the pseudonym key that links samples and data, thereby preventing re-identification.[91] While the author discusses anonymization strictly in the context of pseudonym-key removal in a biobanking setting, more recent literature emphasizes that genetic data may remain inherently identifiable even when with such measures in place. *Alser et al.* (2016) and other authors state that re-identification of genetic data is feasible even when data are pseudonymized or aggregated, due to its inherent identifiability and cross-referencing potential with public datasets.[92] This theoretical risk is

[86] Recital 26 GDPR; *Purtova*, The law of everything. Broad consent of personal data and future of EU data protection law, Law, Innovation and Technology 2018, 45.
[87] Recital 26 GDPR.
[88] EDPB, Guidelines 01/2025 on Pseudonymisation, adopted on 16.01.2025, 3; see also: ECJ C-413/23 P, ECLI:EU:C:2025:723, EDPS v. SRB.
[89] EDPB, Guidelines 01/2025, 2025, 3.
[90] *Marnau/Berrang/Humbert*, Anonymisierungsverfahren für genetische Daten, Datenschutz und Datensicherheit 2018, 83.
[91] *Herbst*, Datenschutz und Datensicherheit 2016, 375.
[92] *Alser et al.*, Can you Really Anonymize the Donors of Genomic Data in Today's Digital World? In: *Garcia-Alfaro/Livraga/Roudier/Soriente (eds.)*, Data Privacy Management, and Security Assurance (DPM 2015, QASA 2015), Lecture Notes in Computer Science (2016), 237–244; see also *Shabani/Borry*, European Journal of Human Genetics 2018, 149-156; *Shabani/Marelli*, Re-identifiability of genomic data and the GDPR, EMBO reports 2019, 1–5.

substantiated for example by the 2024 lawsuit against 23andMe, where the US Attorneys General argued that genetic data, even when claimed to be anonymized, remains too sensitive to be commercialized without explicit informed consent, due to its inherent identifiability and re-identification potential.[93]

3.2.4. Data subject rights in research

Under the GDPR, individuals are granted a wide range of rights aimed at ensuring transparency, control and accountability when their data is being processed. These rights are stipulated in Chapter 3 of GDPR and include rights to access, rectification, erasure, restriction of processing, objection and data portability. The right of access, in particular, should enable data subjects to control the lawfulness of how their personal data is being processed. Controllers are obligated to handle such requests without undue delay and respond transparently.[94]

However, where the processing of personal data is carried out for scientific research purposes, the exercise of these rights may be significantly curtailed. Article 89(1) GDPR allows for derogations from certain data subject rights, provided that appropriate safeguards are in place and the exercise of those rights would seriously impair or make the research objectives unattainable. The safeguards must be in accordance with GDPR and guarantee data minimization. Yet, the GDPR remains vague on what constitutes such safeguards, leaving considerable discretion to Member States and data controllers.[95]

In sum, while the GDPR provides a solid framework for data subject rights, its research exemptions under Article 89 GDPR introduce significant limitations. These limitations are not inherently problematic, provided that they are counterbalanced by meaningful safeguards. However, the current lack of clarification and harmonization poses challenges for both compliance and ethical integrity in EU-based and international research collaborations.

3.3. China: Personal information protection and genetic data laws

The following sections will examine the Chinese regulatory landscape, focusing on the PIPL, the Human Genetic Resources (HGR) Regulations, and their implications for international genetic research. This structure allows for a focused comparison of the EU and Chinese regimes before turning to the operational challenges of international research partnerships.

Data Protection and data privacy in China are not regulated in one comprehensive piece of data protection legislation but rather spread across different regulations and laws. The three core

[93] DataGuidance, USA: AGs sue to prevent 23andMe from selling customer genetic data without consent, https://www.dataguidance.com/news/usa-ags-sue-prevent-23andme-selling-customer-genetic (accessed 01.02.2026).
[94] Article 5 and 12-22 GDPR; Recital 59 and 63 GDPR.
[95] *Staunton et al.*, frontiers in Genetics 2022, 8–9.

legal frameworks related to data protection and data security in China are: the Personal Information Protection Law (PIPL), the Data Security Law (DSL), as well as the Cybersecurity Law (CSL).[96]

In addition to the privacy and data security frameworks, domain-specific laws governing human genetic materials need to be adhered to when processing and transferring genetic material and data. Particularly relevant and in detail discussed in this chapter are the Human Genetic Resources Regulation (HGR-Regulation) as well as the Biosecurity Law.

The next sections examine the most relevant legislative frameworks in detail.

3.3.1. Personal Information Protection Law (PIPL)

The PIPL is China's first dedicated data protection statute, coming into force in 2021. It aims to strengthen data protection as the digital transformation in China and globally is surging.[97] Before the PIPL became effective, data protection regulations were spread throughout numerous norms, laws and regulations.[98] The legislation establishes a framework that governs the processing including collection and transfer of personal information, with particular emphasis on safeguarding individual privacy and national security. [99] The law applies to both domestic and foreign entities that process personal data of individuals located in China.[100] Personal information means any data, whether held electronically or in another form, that can identify an individual, either on its own or in combination with other data.[101]

"Sensitive Personal Information", as defined in Article 28 PIPL, covers data whose exposure or improper handling could lead to discrimination or severe harm to a person's safety or dignity. This data category explicitly includes medical and health data, biometric data, location data and personal data of minors under the age of 14. The handling of sensitive personal information is subject to heightened protection requirements.[102]

The definition of health data is set out in the Information Security Technology – Guide for Health Data Security (GB/T 39725-2020), a non-binding national standard issued by Chinese authorities that outlines best practices for safeguarding personal health data. Article 3.2 of the

[96] DLA Piper, Data Protection Laws in China, https://www.dlapiperdataprotection.com/index.html?c=CN (accessed 01.02.2026).
[97] *He*, When data protection norms meet digital health technology: China's regulatory approaches to health data protection, Computer Law & Security Review 2022, 1.
[98] Ibid, 7.
[99] *Wang/Du*, Cross-Border Health Data Transfer for Scientific Research Purposes in China: Legislation, Practice, and Challenges, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data: A Global Perspective, Perspectives in Law, Business and Innovation, Springer 2025, 190 f.
[100] Article 3 PIPL.
[101] Article 4 PIPL.
[102] Article 28 PIPL.

Guide defines health data as personal health data and electronic information related to an individual's health and medical matters, originating from the processing of personal health information.[103]

Anonymous data is not considered personal data according to the PIPL.[104]

Under the PIPL, the role functionally equivalent to the GDPR "Controller" is referred to as the "Personal Information Processor". This concept should not be confused with the "Processor" as defined in Article 4(8) GDPR. The PIPL defined the Personal Information Processor as "*organizations and individuals that, in personal information processing activities, autonomously decide processing purposes and processing methods".*[105] For the purposes of clarify and consistency, this thesis refers to this role as the "Controller" or "Data Controller".

Under the PIPL seven legal grounds are recognized for the processing of personal information. These include informed consent, necessity for the performance of a contract, compliance with legal duties, emergency response, public interests including journalism, processing of public or lawfully disclosed data and other statutory exceptions.[106] Notably, the PIPL does not recognize legitimate interest of the controller or another party or scientific research as legal grounds.[107] This means researchers must obtain explicit consent when handling personal data for research purposes. For the processing of sensitive data, such as health data, separate consent is required in any case.[108]

With regard to general processing principles, personal data processing must serve clear and legitimate objectives and remain aligned with its intended purpose, while minimizing the impact on the rights and interests of data subjects.[109] Data controllers must transparently provide information to data subjects about the purpose of the data processing, its necessity and the implications it has on their interests and rights.[110]

Certain derogations from data subject rights are nevertheless permitted. When authorized by administrative regulation or law, the right to be informed and make decisions may be restricted.[111] Similarly, the right to deletion may not apply in cases outlined in Article 18(1) and

---

[103] Article 3 Information Security Technology – Guide for Health Data Security (GB/T 39725-2020), issued 14.12.2020, original: http://www.phic.org.cn/zcbz/bzypj/bzgf/gjbz/202408/P020240819570037182147.pdf, English translation: https://www.codeofchina.com/standard/GBT39725-2020.html (accessed 01.02.2026); see also *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 190.
[104] Article 4 PIPL.
[105] *Kennedy*, The "Gold" Standard – China finalises the long-anticipated Standard Contract under the Personal Information Protection Law, Computer Law & Security Review 2023, 2.
[106] Article 13 PIPL.
[107] *Li/Cong/Liu*, Research sunder China's personal information law, Science 2022, 713.
[108] Article 28–29 PIPL.
[109] Article 6 PIPL.
[110] Article 30 PIPL.
[111] Article 44 PIPL.

Article 35 PIPL, such as when data is required for fulfilling legal obligations or statutory duties.[112] In addition, state organs may process personal data without consent when necessary to fulfil statutory duties related to national security, public safety or criminal investigations.[113] However, this exemption is not absolute. The scope, scale and sensitivity of data processing must still be proportionate to the intended purpose of data processing.[114] These exceptions, while narrower and less detailed than those found in the GDPR, reflect the PIPL's attempt to balance individual privacy with broader legal and administrative interests.

3.3.2. Data Security Law (DSL)

The DSL[115] is in effect since September 2021. It complements the PIPL by regulating data processing activities of personal as well as non-personal data within China's jurisdiction and establishes a framework for regulatory oversight and security supervision. The DSL's extraterritorial applicability covers the processing of data outside of Mainland China that compromise public interests, national security or the rights of Chinese citizens and organization. Consequently, foreign entities engaging in business operations targeting China or whose data practices may significantly affect Chinese interests are advised to ensure compliance with the DSL.[116]

To regulate data processing and security, Article 21 DSL mandates a national classification system based on the data's significance to economic and social development and the degree of risk it could pose to national security or public interests if compromised. This top-down classification model is complemented by sector-specific standards.[117]

In October 2024 the Data Security Technology – Rules for Data Classification and Grading (GB/T 43697-2024)[118] took effect, providing the data classification rules and definitions of the relevant data categories in accordance with the PIPL, DSL and CSL.

"Core Data" refers to information that is highly comprehensive, precise, large-scale or deeply detailed within a specific domain, group, or region. If such data is misused or shared unlawfully, it could have a direct impact on political stability and national security.[119] In case a genetic

[112] Article 45 PIPL.
[113] Article 35 PIPL.
[114] Article 6 PIPL.
[115] Data Security Law of the People's Republic of China (DSL), issued 10.06.2021, original: https://www.moa.gov.cn/ztzl/zhnyzxd/zcfg/zybs/flfg/202501/P020250115579606737948.pdf, English translation: http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html (accessed 01.02.2026).
[116] Article 2 DSL; *Chen/Sun*, Understanding the Chinese Data Security Law, International Cybersecurity Law Review 2021, 209-210.
[117] *Chen/Sun,* International Cybersecurity Law Review 2021, 210-211.
[118] Data Security Technology – Rules for Data Classification and Grading (GB/T 43697-2024), issued 21.03.2024, original: https://www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf?mc_cid=b0acb1c7ee&mc_eid=627c47469b (accessed 01.02.2026), English translation available in Appendix 3.
[119] Ibid.

dataset used for research purposes is considered large scale or impacts national security (e.g. national biobank or pandemic response) it is most likely considered Core Data.

"Important Data" includes data revealing data subjects' health, biosafety, genetic and clinical information. Genetic data and HGR will almost always be considered Important Data.[120]

The DSL requires that Important Data undergo a security assessment ahead of being transferred abroad, which is addressed in detail in Chapter 4.[121]

3.3.3. Cybersecurity Law (CSL)

The Standing Committee of the National People's Congress (NPCSC) adopted the Chinese Cybersecurity Law in 2016, and it came partially into effect in 2017, with an 18-month implementation timeline for the data localization rules. This legislation is seen as a cornerstone of China's digital governance, and it has played a crucial role in establishing legal standards for cybersecurity and data protection.[122] The classification of the data controller under the CSL determines the law's applicability and specific security obligations.

Of particular relevance are the roles of Critical Information Infrastructure Operator (CIIO) as well as the Network Operators, as those are subject to heightened security obligations including localization requirements. The concrete definitions are not explicitly outlined in the CSL, instead, their interpretation is delegated to implementing rules.[123] For the purposes of this thesis, particular attention is paid to the obligations applicable to CIIOs.

The "Regulations on Critical Information Infrastructure Security Protections" provide a definition of Critical Information Infrastructure and clarify what qualifies an operator as a CIIO.[124] A "Critical Information Infrastructure" refers to vital digital infrastructure and systems whose compromise could significantly threaten national security, economic stability, essential services and the public good. The Regulations on Critical Information Infrastructure Security Protections highlight examples of industries, such as telecommunication, technology, industry and public services.[125] On 28 October 2025, the legislature adopted amendments to the CSL, which

---

[120] *Chen/Li*, Is cross-border transfer of China's human genetic data an impossible mission? Human Genetics 2025, 3; Appendix G of the Data Security Technology – Rules for Data Classification and Grading (GB/T 43697-2024), issued 21.03.2024, original: https://www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf?mc_cid=b0acb1c7ee&mc_eid=627c47469b (accessed 01.02.2026), English translation available in Appendix 3.

[121] Article 30 DSL.

[122] *Parasol*, AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws, Cambridge University Press 2021, 94-95; *He*, Computer Law & Security Review 2022, 7.

[123] Measures for the Security Assessment of Data Exports, issued 07.07.2022, original: https://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm, English translation: https://www.chinalawtranslate.com/en/exdata-export-security/ (accessed 01.02.2026); *Parasol*, Cambridge University Press 2021, 98–99.

[124] Regulations on Critical Information Infrastructure Security Protections, issued 30.07.2021, original: https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm, English translation: https://www.chinalawtranslate.com/en/Regulations-on-Critical-Information-Infrastructure-Security-Protections/ (accessed 01.02.2026); *Gamvros/Wang,* Data Protection Report, "Am I a CII operator?" – New regulation in China provides more clarity, https://www.dataprotectionreport.com/2021/08/am-i-a-cii-operator-new-regulation-in-china-provides-more-clarity/ (accessed 20.12.2025).

[125] Article 2 Regulations on Critical Information Infrastructure Security Protections.

entered into force on 1 January 2026. The amendments affect fines and penalties, e.g. increasing fines for CIIO to RMB 10 million. Additionally, the amendments broaden the law's extraterritorial scope, to cover any actions by foreign entities that compromise China's overall cybersecurity and not just that affect China's critical information infrastructure, as it has been before.[126]

3.3.4. Sector-specific regulations: HGR Regulations and Chinese Biosecurity Law

In addition to China's overall data protection regime, sector-specific regulation plays a pivotal role in shaping the legal landscape for preclinical research involving genetic data and human biospecimen. Two legislative instruments are particularly relevant in this context: the Human Genetic Resources Regulation (HGR Regulation), including supplementary legislation[127], and the China Biosecurity Law (CBL) [128]. The State Council issued the HGR Regulations in 2019, with the Regulation entering into force on 1 July 2019. By contrast, the NPC Standing Committee adopted the China Biosecurity Law in October 2020, which entered into force on 15 April 2021. The laws are supplemented by several Q&A documents issued by the National Health Commission (NHC) as well as other guidance materials.[129]

The HGR Regulations establish a comprehensive regime for the collection, use, preservation and specifically outbound transfer of human genetic materials and associated data. They introduce strict requirements for foreign collaboration, ethical review and data access, reflecting China's strategic interest in safeguarding its genetic resources.[130] These provisions are particularly significant for international research partnerships, as they impose mandatory submissions to China's National Health Commission (NHC) and grant Chinese institutions active involvement throughout the research lifecycle.[131]

---

[126] Decision of the Standing Committee of the National People's Congress on Amending the Cybersecurity Law of the People's Republic of China, issued 29.10.2025, original: https://www.gov.cn/yaowen/liebiao/202510/content_7046194.htm, English translation: https://www.lawinfochina.com/display.aspx?lib=law&id=45904 (accessed 01.02.2026); DLA Piper, CHINA: Amendments to Cybersecurity Law Effective 1 January 2026, https://privacymatters.dlapiper.com/2025/11/china-amendments-to-cybersecurity-law-effective-1-january-2026 (accessed 03.01.2026); Mayer Brown, China Finalises Amendments to the Cybersecurity Law What Businesses Need to Know Before 1 January 2026, https://www.mayerbrown.com/en/insights/publications/2025/12/china-finalises-amendments-to-the-cybersecurity-law-what-businesses-need-to-know-before-1-january-2026 (accessed 03.01.2026).

[127] 2023 Measures for Ethical Review of Life Sciences and Medical Research Involving Human Beings (2023 Measures), issued 18.02.2023, original: https://www.nhc.gov.cn/qjjys/c100016/202302/6b6e447b3edc4338856c9a652a85f44b.shtml, English translation: https://www.lawinfochina.com/display.aspx?id=40963&lib=law (accessed 01.02.2026); Implementation Rules for the Regulations on the Management of Human Genetic Resources (MOST Implementing Rules), issued 01.06.2023, original: https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/fgzc/bmgz/202306/t20230601_186416.html, English translation: https://www.chinalawtranslate.com/en/Implementation-Rules-for-the-Regulations-on-the-Management-of-Human-Genetic-Resources/ (accessed 01.02.2026).

[128] Chinese Biosecurity Law (CBL), issued 18.10.2020, amended 2024, original: http://www.xinhuanet.com/politics/2020-10/18/c_1126624481.htm, English translation: https://www.lawinfochina.com/display.aspx?id=43149&lib=law (accessed 01.02.2026); see also *Wang/Wang/Zhang*, Bioethics in China's Biosecurity Law: forms, effects, and unsettled issues, Journal of Law and the Biosciences 2021, 2.

[129] The NHC has issued five Q&A documents between April and October 2025, a document containing Frequently Asked Questions, as well as a service guide providing details on licensing and filing requirements. The documents are translated in Appendix 3.

[130] See *McKibbin/Shabani*, The Journal of Law, Medicine & Ethics 2023, 301-312.

[131] Article 7, 18 and 21-24 HGR Regulation.

The CBL complements the HGR Regulations by providing a broader framework for biosafety and bioethics and affirms the state's sovereign authority over all HGR and biological materials within its territory. This aspect underscores the strategic value of these resources and serves as a justification for the introduction of regulatory mechanisms governing the acquisition, storage, utilization and distribution of biological material and HGR.[132] The CBL addresses eight key domains, including epidemic control, laboratory safety, biotechnology governance and the security management of human genetic and biological resources.[133] The latter is of particular relevance to this thesis as it intersects both data protection and ethical oversight in cross-border research.

Together the HGR Regulations and the Biosecurity Law form a sector-specific regulatory framework that not only governs the domestic handling of genetic data but also imposes significant constraints on international collaboration and data sharing. The following sections will address the scope, definitions and obligations embedded in these laws, with a focus on implications for EU-China preclinical research. Transfer-specific requirements under the HGR Regulations and the CBL are addressed in Section 4.5.

3.3.4.1. Definition and scope of Human Genetic Resources (HGR)

The HGR Regulations treat human genetic resources as a matter of public interest and national security.[134] Article 2 of the HGR Regulations define HGR as both the physical materials, such as biospecimen containing genetic substances, genes and genomes ("Human Genetic Material") and the data derived from the human biological samples ("Human Genetic Information").[135] This dual scope ensures that the regulation applies not only to tangible biological samples, such as human tissues, cells or other biospecimen, but also to digital genetic information, which is increasingly important to preclinical research, especially in fields such as Computational Biology[136] or AI driven genomics. Not in scope under the HGR Regulations are medical imaging data, clinical data and protein and metabolic data.[137]

[132] Article 3-4, 36-38 and 53 CBL, see also *McKibbin/Shabani*, The Journal of Law, Medicine & Ethics 2023, 301-312; *Wang/Wang/Zhang*, Journal of Law and the Biosciences 2021, 1-15.
[133] Article 2 CBL.
[134] See Article 1 HGR Regulation.
[135] Article 2 HGR Regulation.
[136] See Carnegie Mellon University, What is Computational Biology, https://cbd.cmu.edu/about-us/what-is-computational-biology.html (accessed 17.08.2025).
[137] Article 2 MOST Implementing Rules.

Following the changes in regulatory oversight of the HGR legal regime from the Ministry of Science and Technology (MOST) to the National Health Commission (NHC), the latter continued the efforts to narrow the scope of what is understood as HGR and ease the compliance procedures in their Guidelines from early 2025.[138]

Certain biological materials, e.g. bodily fluids, swabs and specimens such as urine, feces, serum and plasma are not subject to HGR oversight if they contain only minimal residual genetic content. As a result, these materials can be collected, used and exported without requiring NHC approval.[139] Whole blood, all cell types, tissue samples, semen, blood and bone marrow smears, as well as hair with follicles, still fall within the scope of HGR material. Notable, whole blood drawn from a patient is treated differently than plasma or serum that is transferred from the hospital to laboratories for testing. The latter scenario would not be in scope of the HGR framework.[140] Part II of the Q&A explicitly highlights two specific exemptions from the HGR regulation: (i) commercial human cell lines, which refers to immortalized cell lines used in manufacturing or research that do not include identifiable sample information and (ii) cell-derived Xenografts (CDX). Patient-derived Xenografts (PDX) are explicitly classified as HGR materials, to which the HGR Regulations apply.[141] Immortalized cell lines that are utilized for scientific research are exempted, if associated sample data are removed and they cannot be attributed to an individual.[142] The HGR provisions apply to collecting, utilizing, preserving and making HGR available.[143]

3.3.4.2. Security management of HGR

Chapter IV of the CBL requires all entities handling HGR to implement risk-preventing systems including biosafety protocols, incident reporting mechanisms and contingency plans for data breaches or data misuse.

---

[138] Covington, China's NHC Issues Updated Guidelines on Human Genetic Resources Management, https://www.covingtonblogs.com/2025/04/18/chinas-nhc-issues-updated-guidelines-on-human-genetic-resources-management (accessed 01.02.2026).

[139] Questions IV.1, IV.2 and IV.3. FAQ regarding Human Genetic Resource Management, issued 27.03.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/39a747744f2242068fdaf39b0452e11e.shtml (accessed 01.02.2026), English translation in Appendix 3.

[140] Administrative Licensing for the Collection of Human Genetic Re-sources in China Service Guide, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/3b99b808608240878f866e53ce3a8e36/files/1746832742892_58540.pdf (accessed 01.02.2026), English translation available in Appendix 3.

[141] Q&A on Issues Related to the Management of Human Genetic Resources (Part II), issued 09.04.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202504/17f9863c65c742d4b31ccb745e26082a.shtml (accessed 01.02.2026), English translation available in Appendix 3.

[142] Q&A on Issues Related to the Management of Human Genetic Resources (Part I), issued 01.04.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202504/e9974e2f7a324590947485b74d796b71.shtml (accessed 01.02.2026), English translation available in Appendix 3.

[143] Article 3 HGR Regulation.

3.3.4.3. Domestic data localization and pre-approval requirements

In addition to the localization requirements established in Article 37 CSL, the HGR Regulations and the CBL establish sector-specific duties for the domestic handling of HGR, covering the collection, use, preservation and oversight. These include prior approval or record-filing with the NHC for specified HGR activities, even when HGR are processed exclusively within China. For instance, activities involving sensitive genetic sources (e.g. important genetic families or specific regions) may require approval, whereas purely domestic clinical trials that do not involve the provision of HGR to foreign parties typically proceed via record-filing with the NHC. While these obligations apply independently of any outbound transfer, they may determine whether and under what conditions a transfer could later be permitted.[144]

[144] Article 36-38 and 53 CBL; Article 2, 3, 7 and 21-24 HGR Regulation; Article 14 and 33 MOST Implementing Rules;.

4. Cross-border data transfers, data localization and collaboration requirements

4.1. Introduction to cross-border transfers and collaborations

International data flows are a cornerstone of modern preclinical research, enabling collaborative innovation across borders. In the context of EU-China biomedical partnerships, however, these flows are governed by complex and often divergent legal frameworks. The GDPR prioritizes fundamental rights and data protection continuity across borders. By contrast, the PIPL emphasizes national security and sovereign control, reflecting broader concerns related to industrial policy and geopolitical considerations.

This section examines the legal architecture governing international data transfers, with a particular focus on GDPR Chapter V and PIPL Article 38 and the implications for EU-China preclinical cancer research collaborations. It highlights the mechanisms available to researchers, such as adequacy decisions and standard contractual clauses including transfer impact assessments and explores how these tools interact with sector-specific obligations, including China's HGR Regime and Biosecurity Law.

Additionally, the section addresses requirements for collaborations, including Joint Controllership under Article 26 GDPR, which frequently arise in research collaborations involving several parties. Finally, the section addresses the governance implications of data sovereignty and data localization. While the EU promotes the free flow of data within its internal market and asserts regulatory authority over data processed abroad, China enforces localization mandates for CIIOs and large-scale data. These contrasting approaches create a dual compliance landscape that researchers must navigate.

4.2. EU legal framework for international data transfers and joint controllership

GDPR's chapter V establishes the framework governing the international transfer of personal data, aiming to ensure that the level of data protection guaranteed within the EU is not undermined when data are transferred to third countries or international organizations and processed there. The transfer regime also extends to onward transfers from such third countries, subjecting them to equivalent safeguards.[145]

A data transfer to third countries is only lawful if the recipient country either ensures an "adequate" level of data protection or if appropriate safeguards are in place.

[145] Article 44 GDPR and Recital 101 GDPR.

4.2.1. Adequacy decision under Article 45 GDPR

The European Commission can recognize a country's adequate level of data protection by adopting an adequacy decision based on Article 45 GDPR. Such a decision is adopted following an assessment by the European Commission, an advisory opinion by the EDPB and formal endorsement by representatives of Member States.[146] All countries that are currently recognized as providing an adequate level of data protection are published in the Official Journal of the European Union and listed on the European Commission's website. China is not among those countries.[147] Adequacy decisions are granted based on factors such as legal order, a governing legal framework, access by public authorities to personal data, effective enforcement measures, independent supervisory authorities and international commitment to data protection frameworks. They are evaluated periodically at a minimum interval of four years.[148]

The consequences of such an adequacy decision are that personal data can be transmitted from the European Union and European Economic Area (EEA), including the EEA EFTA States Norway, Liechtenstein and Iceland, to the designated third country without the need of additional safeguards. Essentially, data transfers to those countries are treated equivalently to intra-EEA data transfers.[149]

For outbound data transfers to a third country for which no adequacy decision under Article 45(3) GDPR exists, data may be transferred only if sufficient safeguards are in place. Additionally, individuals must be granted enforceable rights along with access to effective judicial remedy in the recipient country.[150]

The safeguards for international data transfers are listed under Article 46(2) GDPR. The section provides detailed information on the transfer mechanisms under GDPR, most relevant for international research.

4.2.2. Standard Contractual Clauses and Transfer Impact Assessment

Under Article 46(2)(c) GDPR the European Commission can establish standard contractual clauses (EU-SCCs) through the procedure defined in Article 93(2) GDPR. These clauses are recognized as a valid transfer mechanism for ensuring adequate data protection when transferring personal data to countries outside the EEA. According to a survey conducted by IAPP & EY in 2019, EU-SCCs are the most commonly used method of data export from the EU, with 88%

[146] European Commission, Adequacy decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 01.02.2026).
[147] Ibid.
[148] Article 45 (2) and (3) GDPR.
[149] European Commission, Adequacy decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 01.02.2026).
[150] Article 46 (1) GDPR.

of survey-respondents stating that they utilize EU-SCC as a mechanism for outbound data transfers, followed by the – then still valid – Privacy Shield with 60%.[151]

In order for the EU-SCCs to be considered appropriate for safeguarding outbound data transfers, they need to be agreed upon between the data exporter located in the Union and the data importer located in a third country. The content of the EU-SCCs cannot be adapted, besides choosing the relevant modules and options offered, completing placeholders and Annexes or including further safeguards. If the parties wish to modify the core text, they must seek approval from the competent data protection authority for such "ad hoc clauses" pursuant to Article 46(3)(a) GDPR.[152]

While the EU-SCCs remain a valid transfer mechanism for data transfers to any countries lacking an adequacy decision, stricter transfer conditions apply since the Schrems II ruling and relying on EU-SCCs alone is no longer sufficient.[153] Data exporters must assess via a Transfer Impact Assessment (TIA) on a case-by-case basis whether the legal system in the recipient country offers a level of protection that is substantially equivalent to GDPR standards. The assessment shall include whether public authorities, such as intelligence services, have access to the transferred data and whether such access is limited and subject to judicial oversight. Any specific aspects of the transfer should be considered. This ranges from the data flow structure, parties to the processing activities, planned cross-border flows, nature of the recipient and the intended use of the personal data.[154] If the assessment shows that EU-SCCs alone cannot guarantee an adequate level of protection, additional safeguards must be put in place. These range from technical (e.g. encryption), contractual (e.g. transparency obligations towards the data exporter) or organizational (e.g. internal policies) as outlined in the EDPB's Recommendations 01/2020. The EDPB Recommendations further stress the importance of documenting this process carefully and reviewing it regularly. [155] There are several practical guidelines and recommendations on the TIA assessment publicly available.[156] The data transfer must be stopped or omitted in case no suitable measures are available. This shall ensure that the level of protection required under GDPR is maintained, even when data leaves the sphere of the EEA.[157]

---

[151] IAPP-EY, Annual Privacy Governance Report 2019 https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt4eeb51e4cacccc06/Governance_Report_2019.pdf (accessed 07.02.2026), 77.
[152] European Commission, New Standard Contractual Clauses – Questions and Answers overview, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (accessed 01.02.2026).
[153] According to German Data Protection Conference (Datenschutzkonferenz) the new SCCs and TIA stem from case law of the ECJ (See *Durmus*, Praktische Durchführung von Transfer Impact Assessments (TIA), Datenschutz-Berater 2023, 48).
[154] *Golland*, Anforderungen an Transfer Impact Assessments bei Datentransfers in unsichere Drittländer, Datenschutz-Berater 2021, 229.
[155] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18.06.2021.
[156] See *Durmus*, DSB 2023, 48.
[157] EDPB, Recommendations 01/2020, 2021, 4 and 8.

The Commission adopted two new versions of the EU-SCCs on 4 June 2021, merely a year after the CJEU deemed relying solely on the existing EU-SCCs to be not sufficient for securing data transfers to third countries.[158] Besides offering EU-SCCs for governing intra-EU controller and processor relationships for meeting Article 28(3) GDPR requirements, new EU-SCCs according to Article 46(2)(c) GDPR following the Article 93(2) GDPR procedure have been established.[159] The new set of clauses must be used from 27 June 2021 onwards. For existing data transfers the transition period for establishing the new set of clauses has ended on 26 December 2022.[160]

The 2021 EU-SCCs are structured in a modular manner. Depending on the roles of the exporter (party located in the EEA) and the importer (party located outside the EEA) four different transfer constellations can be covered: (1) module 1: controller-to-controller constellation; (2) module 2: controller-to-processor constellation; (3) module 3: processor-to-(sub-)processor constellation and; (4) module 4: processor-to-controller constellation.[161]

4.2.3. Alternative data transfer safeguards

In addition to EU-SCCs, data transfers to third countries lacking an adequacy decision may be based on safeguards provided for in Article 46 GDPR.[162] In its FAQs on the Schrems II judgement, the EDPB clarifies that the CJEU's standard for assessing an essentially equivalent level of data protection applies not only to transfers based on EU-SCCs, but to all transfer mechanisms under Chapter V GDPR.[163] By contrast, a TIA is not required where a data transfer is based on derogations set out in Article 49 GDPR for specific transfer situations.[164] Such derogations must, however, be interpreted restrictively and assessed on a case-by-case basis.[165]

Alternative data transfer mechanisms, namely Binding Corporate Rules, codes of conduct and certifications, approved ad-hoc contract clauses and derogations for specific situations, are set out in the following sections.

---

[158] *Reuter/Voigt*, Die neuen EU-Standardvertragsklauseln - Best Practice, DSB 2022, 309.
[159] *European Commission*, New Standard Contractual Clauses – Questions and Answers overview European Commission.
[160] *Reuter/Voigt*, DSB 2022, 309.
[161] Ibid, 309.
[162] Article 46 GDPR.
[163] EDPB, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, adopted on 23.07.2020, point 2.
[164] CNIL, Transfer Impact Assessment (TIA): the CNIL publishes the final version of its guide, published on 09.07.2025, https://www.cnil.fr/en/transfer-impact-assessment-tia-cnil-publishes-final-version-its-guide (accessed 01.02.2026).
[165] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25.05.2018, 2; EDPB, Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, published 17.07.2020, https://www.edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en (accessed 01.02.2026).

4.2.3.1. Binding Corporate Rules

Pursuant to Article 47 GDPR, Binding Corporate Rules (BCR) may be used to govern international data transfers within a group of undertakings[166] or enterprises engaged in joint commercial activities. The BCRs require prior approval by the competent supervisory authority following the consistency mechanism laid down in Article 63 GDPR.

However, they may be relied upon only after a TIA has been conducted, as BCRs are legally binding solely on the participating entities and their employees. Public authorities, including security agencies, cannot be bound by BCRs, as they are not parties to the internal rules.[167] To be approved, BCRs must meet several requirements outlined in Article 47 GDPR, ranging from detailed explanations on the nature of the data transfers, to reflecting the key GDPR principles[168] and addressing onward data transfers to recipient outside of the BCR framework. For BCRs to be relied upon, they must guarantee enforceable rights to data subjects, including the right to lodge complaints and seek compensation.

The EU-based group entity must accept liability for breaches committed by non-EU entities unless it can demonstrate that it was not responsible for the event, giving rise to the damage.[169] A mandatory component of the BCR consists of procedures for complaint handling, internal audits, training and cooperation with supervisory authorities. The parties to the BCRs must ensure their staff who have regular access to personal data receive appropriate and ongoing training. One key element of BCRs is the duty to inform the supervisory authority where a legal obligation in a recipient country would seriously undermine the safeguards provided for in the BCR.[170] This includes requests by public authorities, such as security or law enforcement agencies, to disclose personal data including situations arising under foreign surveillance legislation.[171]

4.2.3.2. Approved Codes of Conduct and Certification Mechanisms

Approved Codes of Conduct (CoCs) pursuant to Article 40 GDPR, as well as approved certification mechanisms under Article 42 GDPR, may serve as appropriate safeguards for transfers of personal data to third countries within the meaning of Article 46(2)(e) and (f) GDPR.[172] In both cases, they may only be used if the data importer assumes binding and enforceable obligations.[173]

---

[166] Recital 37 GDPR.
[167] CJEU C-311/18, ECLI:EU:C:2020:559, Schrems II, para. 125.
[168] Article 5-11 GDPR.
[169] Article 82(3) GDPR.
[170] Article 47 GDPR.
[171] *Gabauer/Höller*, Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down?, Dako 2020, 80.
[172] Article 40 (3) GDPR; Article 42 (2) GDPR.
[173] *Gabauer/Höller*, Dako 2020, 80.

In the context of preclinical research, Codes of Conduct may constitute a practical and compliant instrument for safeguarding the transfer of research data to entities located outside the EEA. In particular, several sector-specific CoC addressing the processing and transfer of genetic and health data, including for secondary research purposes, are currently under development.[174]

At EU level, the European CRO Federation's GDPR Code of Conduct for Service Providers in Clinical Research has been approved pursuant to Article 40 and 41 GDPR.[175]

In addition, several national supervisory authorities have approved domestic CoCs under Article 40 and 41 GDPR, primarily addressing sector-specific data processing activities within their respective jurisdictions:

- Italy: Veneto Region - Code of conduct for the use of health data for educational purposes and scientific publication[176]
- Poland: Code of Conduct for the Healthcare Sector[177] as well as the Code of Conduct concerning the Protection of Personal Data Processed in Small Medical Facilities[178]
- Spain: Spanish Code of Conduct of the Pharmacy Sector for clinical trials and pharmacovigilance[179]

Matar et al. (2022)[180] proposed a CoC designed to facilitate international genetic data sharing, in their article published in Developing World Bioethics.

4.2.3.3. Approved ad hoc contract clauses

Data transfers to third countries can also be permitted through individually negotiated contracts, provided these are approved by the competent supervisory authority subject to Article 46(3) GDPR. Unlike EU-SCCs, those ad hoc clauses are tailored to the specific circumstances

---

[174] The Innovative Medicines Initiative (IMI) Code of Practice on Secondary Use of Medical Data in Scientific Research Projects was established prior to GDPR under the Data Protection Directive (See Innovative Health Initiative, Code of Practice on Secondary Use of Medical Data in Scientific Research Projects, published 27.04.2014, https://www.ihi.europa.eu/sites/default/files/uploads/documents/reference-documents/CodeofPractice_SecondaryUseDRAFT.pdf (accessed 01.02.2026)); Currently the "Biobanking and Biomolecular Resources Research Infrastructure – European Research Infrastructure Consortium" (BBMRI-ERIC) is working on establishing a "Code of Conduct for Health Research" (See BBMRI-ERIC, A Code of Conduct for Health Research, https://code-of-conduct-for-health-research.eu/ (accessed 20.12.2025).

[175] European CRO Federation, GDPR Code of Conduct, https://eucrof.eu/gdpr-code-of-conduct/ (accessed 01.02.2026); The code is not publicly available, but can requested using the link on the European CRO Federation's website: https://eucrof.eu/gdpr-code-of-conduct/.

[176] Garante per la protezione dei dati personali, Regione Veneto - Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica, published 14.01.2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9535402 (accessed 01.02.2026).

[177] Okręgowa Izba Lekarska w Szczecinie, KODEKS POSTĘPOWANIA DLA SEKTORA OCHRONY ZDROWIA, issued 23.11.2020, https://www.oil.szczecin.pl/upload/files/KODEKS%20POSTEPOWANIA%20DLA%20SEKTORA%20OCHRONY%20ZDROWIA.pdf (accessed 01.02.2026).

[178] Urząd Ochrony Danych Osobowych, The first Polish code of conduct compliant with the GDPR approved, https://uodo.gov.pl/en/553/1325 (accessed 01.02.2026).

[179]Agencia Española de Protección de Datos, Código de Conducta regulador del tratamiento de datos personales, published February 2022, https://www.aepd.es/documento/codigo-conducta-farmaindustria-cc-0007-2019.pdf (accessed 01.02.2026).

[180] *Matar et al.*, A proposal for an international Code of Conduct for data sharing in genomics, Developing World Bioethics 2022, 344-357; this CoC proposal has been funded by the SIENNA project, part of the EU's Horizon 2020 program.

and individually agreed upon by the parties involved.[181] Approvals can be refused if the clauses are not sufficiently governing the transfer.[182] Due to the lengthy approval process and the potential of refusal of such an approval, relying on individual ad hoc clauses may entail significant practical uncertainty.

4.2.3.4. Derogations for specific situations

When neither an adequacy decision, nor any of the other appropriate safeguards as set out in Article 46 GDPR are available, a transfer to a third country may be carried out under one of the exemptions for specific scenarios provided for in Article 49 GDPR. The derogations are designed for very specific and limited circumstances (hence "specific situations") and must be interpreted narrowly. One option is the explicit consent of the data subject that must include transparent information on the potential risks arising from the transfer due to the lack of an adequacy decision or any of the safeguards.[183]

A second option is provided in Article 49(1)(b) and (c) GDPR, which permit a transfer when it is necessary for the performance of a contract, including pre-contractual steps, between the data subject and the controller, or when it is necessary for the conclusion or performance of a contract between the controller and a third party undertaken for the benefit of the data subject.[184] Relying on these derogations is permissible only if the transfer is occasional and genuinely necessary for the performance of the relevant contract or pre-contractual steps.[185]

Other permissible legal grounds for outbound data transfers are compelling public interests stipulated in Union or Member State legislation (Article 49(1)(d) GDPR), legal claims (Article 49(1)(e) GDPR, vital interests (Article 49(1)(f) GDPR and limited public registers (Article 49(1)(g) GDPR).

Finally, transfers are allowed based on necessity and compelling legitimate interests of the controller which must be balanced against the data subjects' interests. This derogation only applies where the transfer is occasional, affects a small number of individuals and additional safeguards are put in place. Additionally, the supervisory authority has to be informed, and the controller must provide the data subject in addition to the information required under Article 13 and 14 GDPR with transparency on the transfer as well as on the specific legitimate interests.[186]

---

[181] *Knyrim/Gerhalter* in: *Knyrim* (Ed.) DatKomm Art 46 DSGVO (2023), para. 70.
[182] *Gabauer/ Höller*, Dako 2020, 80.
[183] Article 49 (1)(a) GDPR.
[184] Article 49 (1)(b) and (c) GDPR.
[185] Recital 111 GDPR; EDPB, Guidelines 2/2018, 2018, 5.
[186] Article 49 (1) subpara. 2-4 GDPR.

4.2.4. EU data transfer decision tree

The following decision tree summarizes the stepwise approach for lawful international data transfers under the GDPR and provides the reader with a concise overview of key transfer considerations.

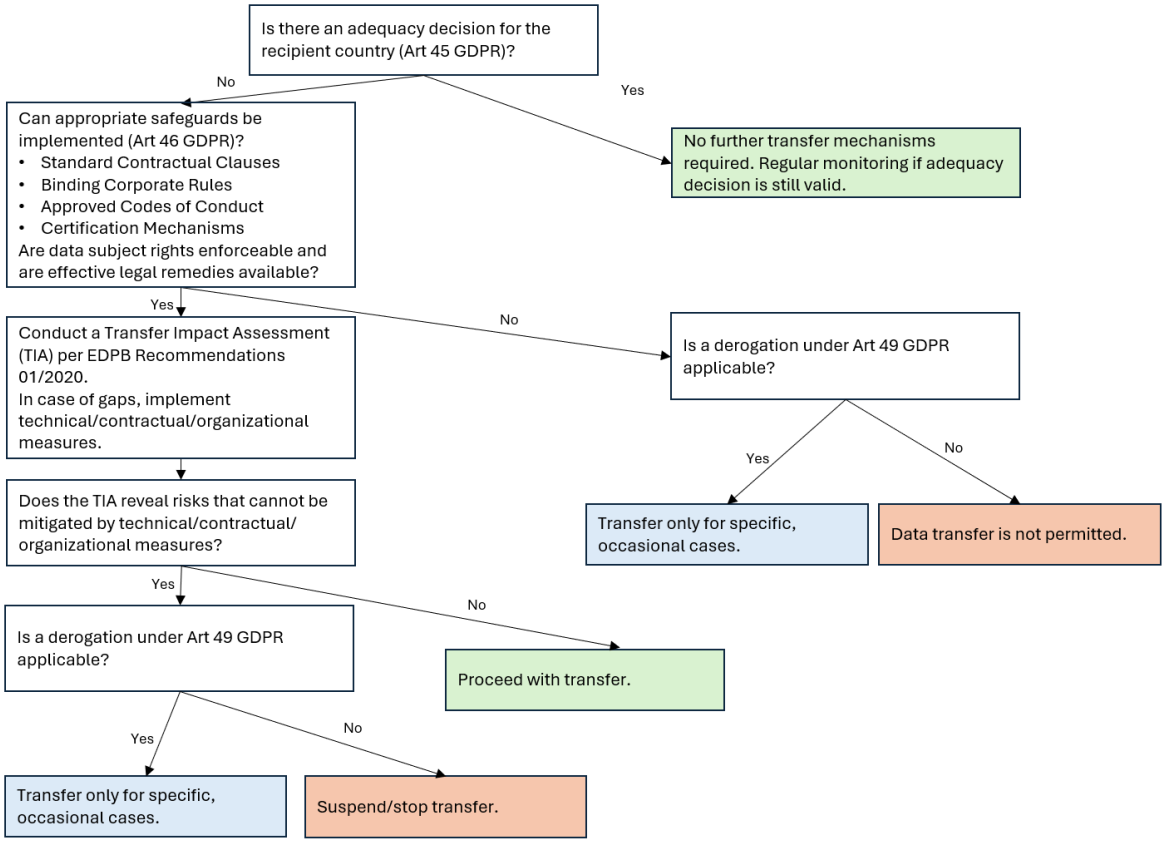

Figure 1: Decision Tree for EU Data Transfers

4.2.5. Joint Controller Agreement (JCA)

Regardless of any data transfers, the GDPR mandates in Article 26 GDPR the conclusion of a Joint Controller Agreement (JCA), in case multiple parties jointly decide on the aims and methods of processing personal data. In such a case the parties are considered Joint Controllers.[187] Practical implications related to the JCA are analyzed in Chapter 5.

Under Article 26(3) GDPR, read in conjunction with Article 82(4) GDPR, joint controllers are subject to joint and several liability where a GDPR breach causes damage, subject to exemption from liability if one controller can demonstrate that it is not in any way responsible for the event giving rise to the damage.[188] Conversely, where one party strictly follows the docu-

[187] Article 26 GDPR.
[188] Article 82(4) GDPR.

mented instructions of another and does not influence the purpose or essential means, a controller-processor constellation is indicated and should be governed by Article 28 GDPR, rather than Article 26 GDPR.

The Court of Justice has repeatedly emphasized that joint controllership is a functional concept, not dependent on formal labels or equal degrees of influence. Even limited, but "*decisive influence on the purposes and means*"[189] may suffice to qualify an entity as a joint controller.[190] Recent case law has also shown that joint controllership may exist for specific phases of a broader processing chain, while other phases remain outside their joint determination.[191] In research collaborations, role analysis should therefore be granular, e.g. by dataset and processing step, and documented before any data sharing occurs.

The JCA could potentially reflect internal indemnity and cost-sharing arrangements consistent with Article 82 GDPR and clarify procedures for handling complaints (Article 77–79 GDPR), supervisory authority investigations (Article 58 GDPR) and fine-related considerations.[192]

4.3. China's Cross-Border Data Transfer (CBDT) regime

4.3.1. Key laws and regulations governing CBDT

The PIPL, as well as other laws and regulations, cover legal requirements related to data transfers out of the territory of Mainland China. Those are specifically:

- Personal Information Protection Law (PIPL) in force since 01. November 2021 covers general principles for CBDT.
- Measures for the Security Assessment of CBDT in force since 01. September 2022 governing the security assessment, relevant thresholds and procedures.
- Measures on Contracts for the Export of Personal Information (SC Measures) in force since 01. June 2023 and establishing Chinese SC, thresholds for filing with the CAC and the formal procedure related to the Chinese SC.[193]

[189] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 20.07.2021, para. 30.
[190] CJEU C-604/22, ECLI:EU:C:2024:214, IAB Europe, para. 58-59.
[191] CJEU C-604/22, ECLI:EU:C:2024:214, IAB Europe, para. 71.
[192] Article 58 GDPR, Article 77-83 GDPR; EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1, adopted on 24.05.2023.
[193] Measures on Standard Contracts for the Export of Personal Information (SC Measures), issued 03.02.2023, original: https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm, English translation: https://www.chinalawtranslate.com/en/personal-information-export-contract/ (accessed 01.02.2026).

- Provisions on Promoting and Regulating the Cross-Border Flow of Data, in force since 22 March 2024, govern the data export oversight and exemptions from transfer restrictions.[194]
- Free-Trade Zone's CBDT Rule issued on 30. August 2024 (Beijing FTZ Data Outbound Negative List) and 08. February 2025 (Shanghai FTZ Data Export Negative List) implementing sandbox areas for further simplification of CBDT requirements via elevated thresholds for specific industries, such as the pharmaceutical industry.[195]

The PIPL has introduced strict rules governing the cross-border transfer of personal data. If personal data are intended to be transferred out of China, one of four transfer mechanisms must be used:

(1) passing a Security Assessment organized by the State Cyberspace Administration of China (CAC) (Article 38(1) and in accordance with Article 40 PIPL);
(2) concluding a Standard Contract for Cross-border Transfer of Personal Information with the data importer, using the template provided by the CAC[196];
(3) obtaining certification from an institution accredited by the CAC[197]; or
(4) relying on other transfer mechanisms as provided by applicable laws or regulations or as determined by the CAC.[198]

Requirements and thresholds for the different transfer mechanisms are regulated in various administrative regulations such as the Critical Information Infrastructure Security Protection Regulations[199], the Measures for the Security Assessment of Data Exports[200], the Provisions on Promoting and Regulating Cross-border Data Flows[201], as well as the Measures on Standard Contracts for the Export of Personal Information (SC Measures)[202].[203]

---

[194] Provisions on Promoting and Regulating the Cross-Border Data Flows, issued 22.03.2023, original: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm, English translation: https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/.
[195] Beijing FTZ Data Outbound Negative List, issued 30.08.2024, original: https://www.beijing.gov.cn/zhengce/zhengcefagui/202409/t20240902_3787646.html, no English translation available, English summary: https://english.beijing.gov.cn/investinginbeijing/two_zones/updates/202409/t20240914_3891329.html (accessed 01.02.2026); Shanghai FTZ Data Export Negative List.
[196] Standard Contract for Cross-border Transfer of Personal Information, https://www.glo.com.cn/UpLoadFile/Files/2023/3/1/11535343a7a943e1-f.pdf (accessed 01.02.2026).
[197] The certification seems to be intended to facilitate data transfers within a group of companies, similarly to Binding Corporate Rules under GDPR; See *Kennedy*, Law, Computer Law & Security Review 2023, 1.
[198] Article 38 PIPL.
[199] Regulations on Critical Information Infrastructure Security Protections.
[200] Measures for the Security Assessment of Data Exports.
[201] Provisions on Promoting and Regulating the Cross-Border Flow of Data, issued 22.03.2024, original: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm, English translation: https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/ (accessed 01.02.2026).
[202] Measures on Standard Contracts for the Export of Personal Information (SC Measures), issued 03.02.2023, original: https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm, English translation: https://www.chinalawtranslate.com/en/personal-information-export-contract/ (accessed 01.02.2026).
[203] See *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 190-209.

When personal data are shared with a foreign data recipient, the data controller must additionally acquire separate, purpose-specific consent of the affected individuals and must inform them about particular aspects of the data processing. The information must include the name as well as contact details of the foreign recipient, purpose and methodology of processing, affected data categories and the procedures by which they can exercise their rights under the PIPL vis-à-vis the foreign recipient.[204]

4.3.2. Security evaluation approval by the CAC

In 2024, the Cyberspace Administration of China (CAC) adopted the Provisions on Promoting and Regulating the Cross-Border Flow of Data (CBDF Provisions), which clarify the circumstances under which Chinese parties must rely on a CAC-organized security assessment for cross-border data transfers in accordance with Article 40 PIPL.[205] Any Critical Information Infrastructure Operator (CIIO)[206] transferring personal information or critical data abroad must seek prior security evaluation approval. Critical Data, also known as Core Data, includes information that, if compromised, could pose risks to national security, public safety, economic stability or social order.[207] Additionally, where a non-CIIO data controller transfers either critical data or personal data (not including sensitive data) relating to more than 1 million individuals or sensitive data of more than 10.000 individuals, such an approval is also required.[208]

Before data controllers apply for a security assessment, they must conduct a self-assessment to identify and assess potential threats that may arise in the context of cross-border data transfer.[209]

The Q&A on Data Cross-Border Security Management Policies issued by the CAC clarifies that "General Data", information that is neither personal data nor classified as Important or Core Data, may be transferred internationally without additional regulatory procedures. The Q&A

[204] Article 39 PIPL.
[205] Provisions on Promoting and Regulating the Cross-Border Flow of Data; *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 190-191.
[206] "Critical Information Infrastructure" is defined in Article 2 Regulations on Critical Information Infrastructure Security Protections and covers key network infrastructure and information systems across vital sectors such as telecommunication, energy, finance, transportation, public services and national defense (see *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 208-209).
[207] Definitions are stated in Data Security Technology – Rules for Data Classification and Grading (GB/T 43697-2024); see *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 191-192.
[208] Article 7 of the Provisions on Promoting and Regulating Cross-border Data Flows; See *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 208-209
[209] Ibid; Article 5 Measures for the Security Assessment of Data Exports.

also introduces practical reliefs. Corporate groups are permitted to submit consolidated applications. Additionally, the validity of approved security assessments can be extended from 2 to 3 years under certain conditions.[210]

4.3.3. Chinese Standard Contract

On 24 February 2023 the CAC has issued the long-anticipated Measures on Standard Contracts for the Export of Personal Information (SC Measures), including the template for the Chinese Standard Contract.[211] The controllers that base their transfers on the Standard Contract are required to review their transfer processes within the transition period in order to fulfill the obligations under the PIPL and the SC Measures. *Kennedy* (2023)[212] argues that she expects the Standard Contract to be the most relevant transfer mechanisms moving forward.

The SC Measures clarify that the Standard Contract may be used only where all of the following conditions are met: (i) the data controller is not classified as a CIIO; (ii) it processes personal data relating to fewer than 1 million individuals in total; and (iii) since 1 January of the preceding year, it has transferred personal data relating to fewer than 100.000 data subjects or sensitive data relating to fewer than 10.000 individuals.

Additionally, there might be scenarios where laws and regulations specifically require utilization of other transfer mechanisms. Segmenting data transfers into smaller batches in order to bypass the mandatory security assessment is prohibited under Article 3 SC Measures, but it is unclear under which exact conditions such a segmentation would be considered illegitimate.[213]

The Standard Contract specifies that separate consent must be obtained for any outbound transfer of personal data. For data subjects under the age of 14, parents or legal guardians can consent on behalf of the minor.[214] Additionally controllers are also required to inform individuals of their third-party beneficiary rights, which become effective if the data subject does not object within 30 days.[215]

The Chinese data controller must further ensure and take reasonable steps to confirm that the foreign data importer implements adequate data protection measures. The Standard Contract

---

[210] Question 1, 8 and 9 Q&A on Data Export Security Management Policies, issued 09.04.2025, original: https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm (accessed 01.02.2026), English translation available in Appendix 3; *Huld,* China Clarifies Cross-Border Data Transfer Rules: Key Takeaways from Official Q&A (I), China Briefing, https://www.china-briefing.com/news/china-clarifies-cross-border-data-transfer-rules-official-qa/ (accessed 05.10.2025).
[211] The SC Measures are in effect since 1 June 2023, including a 6-month long grace period, for any transfers established prior to 1 June 2023; Article 13 SC Measures; Standard Contract for Cross-border Transfer of Personal Information (See *Kennedy*, Law, Computer Law & Security Review 2023, 2).
[212] Ibid, 1.
[213] *Kennedy*, Law, Computer Law & Security Review 2023, 1.
[214] Article 2(3) Standard Contract.
[215] Article 5 SC Measures; Article 2(4) Standard Contract.

specifically mentions TOMS, such as encryption, anonymization, de-identification and access control measures.

The Standard Contract must be used without modifications unless this is explicitly permitted by the CAC. Supplementary clauses might be added only in case they do not contradict the core provisions of the Standard Clauses.[216] This means that companies that already have existing contracts in place, such as Data Processing Agreements or Intercompany Data Transfer Agreements, must revise those in order to ensure alignment with the updated regulatory framework.[217]

The controller has to submit the Standard Contract, as well as the mandatory Personal Information Protection Impact Assessment (PIPIA), to the respective authorities within 10 working days after the Standard Contract has become effective.[218] The authority does not formally approve the documents, as the data controller is liable for the accuracy of the filed records.[219] In case of any changes to the processing activity and data transfer affecting core aspects, the Standard Contract as well as the PIPIA has to be redone and filed with the regulatory authority again. Core aspects in this regard are considered the purpose, scope, sensitivity or retention of the exported personal data, significant adaptations to the legal framework of the importing country affecting the data subjects' rights or any other developments affecting data protection rights.[220]

Concluding the Standard Contract obligates the foreign data importer to (i) implement TOMs (encryption, access controls, de-identification), (ii) assist the exporter in fulfilling data subject rights, (iii) notify the exporter of government access requests or conflicting laws and (iv) being subject to Chinese supervisory oversight where applicable.[221]

4.3.4. Certification by accredited institutions

Certifications by accredited institutions, as established under Article 38 PIPL, offer an alternative mechanism for legitimizing the transfer of personal information outside of China. The "Implementation Rules for Personal Information Protection Certification" define standards for obtaining certifications. A controller aiming at acquiring a certification for cross-border data handling must comply with the requirements established via the "Security Certification Specifications on Cross-Border Processing of Personal Information v2.0" (TC260 Guidelines).[222] The TC260 Guidelines demand joint legal accountability, regular compliance audits, openness to

[216] Article 6, SC Measures; Article 9(1) Standard Contract.
[217] *Kennedy*, Law, Computer Law & Security Review 2023, 2.
[218] Ibid, 2-3; The PIPIA is discussed in Section 4.3.5.
[219] Ibid 2; Article 8 SC Measures.
[220] *Kennedy*, Computer Law & Security Review 2023, 2.
[221] See SC Measures; Article 2-9 Standard Contract.
[222] See *Guo/Li*, Cross-border data flow in China: Shifting from restriction to relaxation? Computer Law & Security Review 2025, 6.

regulatory supervision, respect for individuals' rights and documentation of all cross-border data activities.[223] While certification can streamline compliance for routine operational data, it does not replace sector-specific approvals and export controls for genetic material and derived information, which remain subject to HGR Regulations and mandatory Chinese partner involvement.[224]

4.3.5. Personal Information Protection Impact Assessment (PIPIA)

The Chinese legislation mandates conducting a Personal Information Protection Impact Assessment (PIPIA) in certain circumstances. When personal data are transferred abroad and based on a security review organized by the CAC, a certificate by an accredited institute or on a Standard Contract, a PIPIA is mandated.[225] This assessment has to be documented and records are stored for at least three years.[226]

The PIPIA must include an assessment of various key aspects ranging from assessing the lawfulness, necessity and proportionality of the processing purpose, to the nature, volume and sensitivity of the data and associated risks to the affected individuals. Further, the data importers capacity to fulfill data protection obligations through adequate TOMs, the potential for data being compromised and the availability and mechanisms to uphold data subjects' rights, the influence of the foreign jurisdiction's legal framework on contract enforceability and any additional elements that may affect data security must be considered for the assessment.[227]

The essence of the PIPIA slightly differs depending on the transfer mechanisms utilized and is regulated in the respective Implementing Rules.[228]

---

[223] Article 5.1(j), Article 5.2.2(e), Article 6.1(d), article 6.1(f), Article 6.2(f) TC260 Guidelines cited by *Mok,* Secretariat of the National Information Security Standardization Technical Committee, Cybersecurity Standard Practice Guidelines: Specifications for the Security Certification of Cross-Border Personal Information Processing Activities V2.0 (Draft for Comments), China Law & Practice 2022, https://www.proquest.com/docview/2737578271?parentSessionId=eLb%2BAjUO%2FbVCdzAc5ykU15ronhaMRn1PZ%2Bs4a%2F1Bol0%3D&pq-origsite=primo&accountid=14682&sourcetype=Trade%20Journals (accessed 01.02.2026).

[224] Article 7 CAC Provisions; Article 21-22 HGR Regulation; *Chen/Li*, Human Genetics 2025, 3-4; *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Springer 2025, 192-193.

[225] A PIPIA is mandatory if sensitive personal data is processed, data is used for making automated decisions, data processing is delegated, data is shared or disclosed or transferred abroad or in any other processing circumstances that significantly affect data subjects' rights and freedoms. (Article 55 PIPL; see *Huld,* How to Conduct a Personal Information Protection Impact Assessment in China, https://www.china-briefing.com/news/how-to-conduct-a-personal-data-impact-assessment-in-china/ (accessed 03.01.2026).

[226] Article 2(5), 2(7) and 2(8)(iii) Standard Contract.

[227] Article 56 PIPL; *Kennedy*, Law, Computer Law & Security Review 2023, 2; Article 7 SC Measures.

[228] See for example Article 5 SC Measures; *Huld,* How to Conduct a Personal Information Protection Impact Assessment in China, https://www.china-briefing.com/news/how-to-conduct-a-personal-data-impact-assessment-in-china/ (accessed 03.01.2026).

4.3.6. Other legal bases, recent regulatory clarifications and Free Trade Zones

Beyond the main mechanisms for cross-border data transfers, Article 38(4) PIPL provides that transfers may also rely on "*other conditions required by law, administrative regulations or the CAC*".[229]

The CBDF Provisions introduce several exemptions and administrative simplifications. General Data – that is, data which is neither personal nor classified as Important or Core Data – may now be transferred internationally with fewer formalities when processed in contexts such as academic collaborations, marketing or production and manufacturing.[230] Data that benefits from these relaxed requirements includes, for example, CDX model data, as such xenograft models are typically generated from established commercial or public cell lines and do not contain donor-related information.[231] Data not initially generated or collected in China can also be transferred without outbound data transfer restrictions.[232]

The CAC's Q&A on Data Export Security Management Policies issued in April 2025 further clarifies that consolidated applications are permitted for multinational corporate groups.[233] These clarifications reduce administrative burden for large research consortia or pharmaceutical companies with China-based entities collaborating internationally. Further, the Q&A states that the validity of approved security assessments can be extended under specific circumstances from 2 to 3 years,[234] providing greater stability and predictability for long-term research collaborations that involve cross-border flow of data.

In addition, the regulatory framework now grants Free Trade Zones (FTZs) a unique role in facilitating cross-border data flows. FTZs may establish their own negative lists identifying data categories that trigger compliance procedures for export.

Personal data that is not included on those lists may generally be transferred internationally subject to reduced regulatory requirements. This approach, clarified in the CAC's 2025 Q&A, shall harmonize and streamline data export requirements across different FTZs, reducing redundant compliance efforts for research and business data that is not classified as personal or important. As more FTZs publish and implement negative lists, covering a growing range of sectors, research institutions and companies operating within these zones benefit from a more

[229] Article 38(4) PIPL; *Guo/Li,* Computer Law & Security Review 2025, 5.
[230] Article 3 CBDF Provisions; *Guo/Li*, Computer Law & Security Review 2025, 5.
[231] *Das/Das* in: *Pathak/Banerjee/Bisgin* (eds.), Handbook of Animal Models and its Uses in Cancer Research, 503-504; Covington, China's NHC Issues Updated Guidelines on Human Genetic Resources Management, https://www.covingtonblogs.com/2025/04/18/chinas-nhc-issues-updated-guidelines-on-human-genetic-resources-management (accessed 01.02.2026).
[232] Article 4 CDBF Provisions; *Guo/Li*, Computer Law & Security Review 2025, 7.
[233] See Question 8 Q&A on Data Export Security Management Policies.
[234] See Question 9 Q&A on Data Export Security Management Policies.

predictable and efficient pathway for lawful international data transfers, provided the data does not fall under restricted categories.[235]

These changes are intended to reduce redundant compliance burdens and support international business operations. However, it is important to note that these exemptions do not apply to Important Data or CIIO data which remain tightly regulated. The flexibility also does not override sector-specific requirements for HGR or sensitive health data, which remain subject to strict approval and compliance obligations. [236]

In practice, controllers should carefully segment data flows and document the legal basis for each transfer, ensuring that any reliance on these alternative transfer mechanisms is supported by current CAC guidelines and does not conflict with HGR or biosecurity regulations.[237]

4.3.7. Decision tree for Chinese data export requirements

The following decision tree illustrates the regulatory steps for cross-border data transfers from Mainland China:

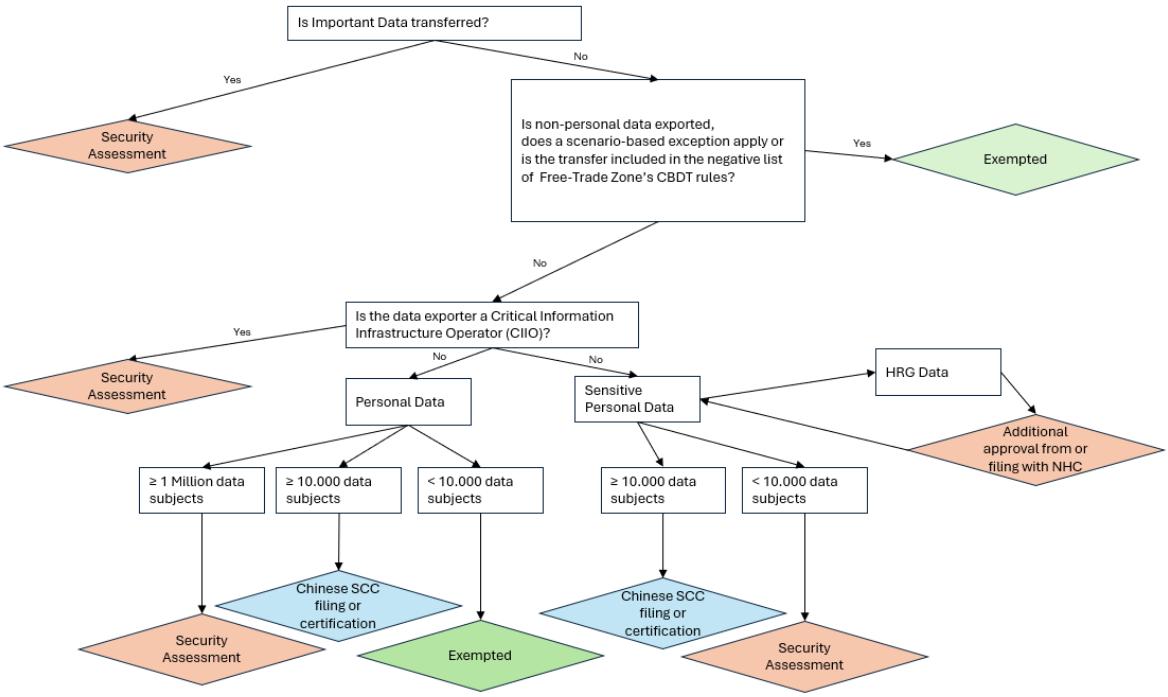

Figure 2: Decision Tree for China's Data Export Requirements

[235] See Question 2 and 3 Q&A on Data Export Security Management Policies; Article 6 Provisions on Promoting and Regulating Cross-Border Data Flows.
[236] See Article 1-5 HGR Regulations and MOST Implementing Rules.
[237] See Article 3-6 Measures for the Security Assessment of Data Exports.

4.4. Cross-border data flow communication mechanism

Recent developments in EU-China data governance have led to the establishment of a formal Cross-Border Data Flow Communication Mechanism, intended to facilitate dialogue and practical solutions for international data transfers. In August 2024, the EU and China launched this mechanism with the aim of addressing regulatory uncertainties and enhancing administrative coordination for cross-border data flows, particularly in sectors such as research and innovation.[238]

The mechanism seeks to promote greater transparency and predictability for organizations engaging in cross-border collaborations. According to the European Commission, it provides a structured platform for exchanging information on regulatory changes, discussing sector-specific challenges and clarifying compliance requirements for data transfers between the EU and China. [239]

While the mechanism does not create legally binding obligations or alter existing legal requirements, it reflects an effort to support regulatory dialogue and administrative cooperation. In this sense, the initiative signals a shared interest in balancing data protection objectives with the practical needs of scientific and economic collaboration, without modifying the underlying legal framework applicable in either jurisdiction.

4.5. Sector-specific transfer restrictions and collaboration requirements

4.5.1. Collaboration requirements

Chinese law imposes strict collaboration requirements for any research involving Human Genetic Resources. These requirements are sector-specific and an important compliance instrument for any international research partnership. Non-domestic organizations ("Foreign Cooperating Parties")[240] are banned from utilizing Chinese HGR[241] except where they cooperate with a domestic scientific research institute, medical institute or academic institute ("Chinese Cooperating Party"). [242] Both parties must jointly apply for approval with the NHC and must indicate the methods used to lawfully acquire HGR.[243] In case data are newly derived from HGR material during the collaboration, no additional filing is needed.[244]

---

[238] European Commission, EU and China launch Cross-Border Data Flow Communication Mechanism, https://policy.trade.ec.europa.eu/news/eu-and-china-launch-cross-border-data-flow-communication-mechanism-2024-08-28_en (accessed 20.12.2025).
[239] Ibid.
[240] This includes institutions founded or governed by such a non-domestic organization or person (Article 21 HGR Regulation).
[241] „utilizing" includes the collection, preservation and abroad provision of Chinese HGR (Article 21 HGR Regulation).
[242] Article 21 HGR Regulation; A "foreign entity" is defined as either being established or being effectively controlled by offshore parties. Control is hereby defined as holding over 50 percent shares of having decisive influence over strategic decisions, even via contractual arrangements (See Article 12 MOST Implementing Rules).
[243] Article 33 MOST Implementing Rules; Article 22 HGR Regulations.
[244] Article 36 MOST Implementing Rules.

Depending on the circumstances, the collaborations are either formally approved by the NHC or have to be notified to the regulator. In an effort to simplify regulatory procedures, the NHC provided exemptions from the approval requirement in the 2025 FAQ document. If the foreign cooperating party is responsible solely for electronic data capture services, approval or notification to the NHC is not needed. Similarly, when a foreign entity sponsors a clinical trial, e.g. by providing the investigated active ingredient or financial support for the trial, without engaging in the exchange of research data, the approval and notification can be dismissed.[245]

A requirement for international research collaboration is that the activity does not impose a threat to public health and national security or public interests in China, and the HGR used are sourced through legitimate channels. In addition, each party must obtain ethics review approval in accordance with the requirements applicable in its respective country or region.[246]

Additionally, it is mandated that any information, data and records created from Chinas HGR must be unrestricted accessible to the Chinese Cooperating Party and a backup copy must be provided to them. Chinese researchers and institutions must be actively involved throughout the entire research process.[247] Within six months after the expiration of the authorization, the Chinese party must continue to provide information to the authority concerning aspects such as the use and disposal of HGR in China as well as the use, recording and storage of all data collected during the research collaboration.[248]

Based on those requirements, it can be argued that they primarily serve to ensure state oversight over genetic material and data. This governance model entails extensive access and involvement rights for the Chinese cooperating party, with implications for data protection, intellectual property management and the degree of state influence over research activities.

4.5.2. Sectoral transfer restrictions

China's regulatory framework for HGR imposes strict sector-specific restrictions that operate in addition to the general mechanisms. The 2019 HGR Regulation, together with the MOST Implementing Rules[249], establishes that any transfer of HGR materials or HGR-derived data abroad requires prior approval or filing with the competent Chinese authority, currently the National Health Commission (NHC).[250]

---

[245] Question II.5, II.6 and II.7 FAQ regarding Human Genetic Resource Management; Covington, China's NHC Issues Updated Guidelines on Human Genetic Resources Management, https://www.covingtonblogs.com/2025/04/18/chinas-nhc-issues-updated-guidelines-on-human-genetic-resources-management (accessed 01.02.2026).
[246] Article 22 HGR Regulation.
[247] Article 14 MOST Implementing Rules.
[248] Article 22 HGR Regulation; Article 35 MOST Implementing Rules.
[249] Implementation Rules for the Regulations on the Management of Human Genetic Resources (MOST Implementing Rules), issued 01.06.2023, original: https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/fgzc/bmgz/202306/t20230601_186416.html, English translation: https://www.chinalawtranslate.com/en/Implementation-Rules-for-the-Regulations-on-the-Management-of-Human-Genetic-Resources/ (accessed 01.02.2026).
[250] *Chen/Li*, Is cross-border transfer of China's human genetic data an impossible mission? Human Genetics 2025, 3-4.

Sharing HGR from China abroad is only permissible in the following scenarios:

(i) Open access is granted to the foreign party by the Chinese party that owns the data. A prerequisite for this constellation is the filing of the collaboration with the NHC by the Chinese party owning the HGR, as well as the provision of any transferred data as a backup to the competent authority. In this context, a lawful basis and the necessity for each proposed activity involving HGR data must be demonstrated. The filings further include a self-evaluation assessing and documenting the potential risk associated with the data being disclosed or transferred to the foreign party.[251]

(ii) The sharing of HGR data is an aspect of the cross-border research collaboration that has been officially authorized.[252]

The NHC is required to conduct a security review in specified circumstances including where HGR of Important Biological Families are provided abroad, where HGR stem from sensitive places or where exome or genome sequencing data relating to more than 500 individuals are shared as well as in other situations that could affect public health, compromise national security or undermine the state's social interests.[253] Where HGR additionally meet the definition of Important Data under Chinese law, a CAC security assessment may be required in parallel, as set out in the 2024 Provisions.[254] The Q&A on Data Export Security Management Policies confirms that the regulatory framework for cross-border transfers is limited to personal information and Important Data. For the identification of Important Data in biotechnology and genetics, it refers to Appendix G of the Data Security Technology – Rules for Data Classification and Grading.[255]

These requirements apply regardless of whether the data qualify as personal information under the PIPL. Accordingly, compliance with the general cross-border data transfer regime does not exempt research actors from compliance with HGR-specific controls.[256] The scope of these restrictions is defined broadly, encompassing both the use and cross-border transfer of Human Genetic Resources.

---

[251] Article 36 MOST Implementing Rules.
[252] Article 27 and 28 HGR Regulations.
[253] Article 37 MOST Implementing Rules; *McKibbin/Shaban*, Journal of Law, Medicine & Ethics 2023, 304; "Important genetic families" are defined as blood-related individuals, where hereditary diseases or genetic traits (excluding common conditions such as diabetes or hypertension) continue over at least three generations within the family (Article 27(1) Implementation Rules; Administrative Licensing for the Collection of Human Genetic Resources in China Service Guide, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/3b99b808608240878f866e53ce3a8e36/files/1746832742892_58540.pdf, English translation available in Appendix 2); "HGR of specific regions" describe HGR of populations that lived isolated or in unique environments over a long period of time and have developed distinct physiological traits or adaptive characteristics (Article 27(2) Implementation Rules; Administrative Licensing for the Collection of Human Genetic Re-sources in China Service Guide, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/3b99b808608240878f866e53ce3a8e36/files/1746832742892_58540.pdf, English translation available in Appendix 2).
[254] Article 7 Provisions on Promoting and Regulating the Cross-Border Flow of Data.
[255] Question 1 and 5 Q&A on Data Export Security Management Policies.
[256] Ibid.

Any export of HGR, whether for collaborative research, commercial use or other purposes, trigger obligations to obtain regulatory approval. Notably, the implementing rules clarify that certain categories of biomedical data, such as routine clinical records or imaging, are not classified as HGR information and may be transferred under the general data protection framework, provided they do not contain or reveal genetic sequence data.[257]

Pilot programs in Chinese Free Trade Zones (FTZs) have introduced industry-specific pilot measures, including for the biopharmaceutical sector. FTZs such as Shanghai have published negative lists that specify which categories of data may be exported subject to reduced regulatory requirements. However, these pilot measures do not override the core localization requirements for Important Data and their practical impact on preclinical cancer research remains limited and continues to evolve in practice.[258]

The Biosecurity Law reinforces these controls by framing HGR as a strategic national asset, subjecting transfers to risk-based scrutiny and, where relevant, security review. This means that even where general outbound transfer provisions or Free Trade Zone exemptions might otherwise apply, HGR-related transfers remain highly regulated and require separate handling.[259] In practice, this dual-track approach obliges researchers to segment data flows and ensure that any transfer involving HGR is supported by the necessary approvals and with documentation of the legal basis for each transfer.[260]

In summary, the sector-specific transfer restrictions for HGR and related bioscience data in China create a parallel compliance regime that must be addressed independently of general data transfer mechanisms.[261]

4.6. Data sovereignty and data localization requirements

"Data Sovereignty" refers to a regulatory concept under which states assert authority over data governance through domestic and regulatory frameworks, particularly where data processing is perceived to implicate national interests, security or public order. The manner in which data sovereignty is governed is inherently different in China and in the EU.[262] While the EU's regulatory framework is fundamentally oriented towards enabling the free movement of data

[257] Question 1 and 5 Q&A on Data Export Security Management Policies.
[258] Article 6 Provisions on Promoting and Regulating the Cross-Border Flow of Data; International Services Shanghai, New list to aid outbound data flows, https://english.shanghai.gov.cn/en-Latest-WhatsNew/20240520/e66e1b5b4f894f6b9c6c1f1dcecc0a76.html (accessed 20.09.2025).
[259] *Chen/Li*, Is cross-border transfer of China's human genetic data an impossible mission? Human Genetics 2025, Human Genetics 2025, 3-4, 7; *McKibbin/Shaban*, Journal of Law, Medicine & Ethics 2023, 303-304.
[260] Ibid.
[261] Ibid.
[262] See *Chen*, Research on Data Sovereignty Rules in Cross-border Data Flow and Chinese Solution, US-China Law Review 2021, 261-263; *Yun*, China's Data Sovereignty and Security: Implications for Global Digital Borders and Governance, Chinese Political Science Review 2025, 178-181.

within the internal market[263], China's data laws impose stringent rules on sharing personal information across borders. Specifically, the DSL, CSL and the PIPL implement a regulatory framework for data sovereignty that treats domestic data storage as a regulatory baseline, with cross-border data transfers permitted only under defined and closely supervised conditions.[264] In this frame, policy objectives extend beyond privacy or cybersecurity to national security, economic competitiveness and strategic autonomy, with exclusive national control and asymmetric access pursued as policy goals.[265]

4.6.1. The EU perspective

The EU grounds its data governance framework on the protection of fundamental rights, with comprehensive data protection laws serving as the primary regulatory instrument.[266] Within the Union, there is no overarching legal requirement to store research or health data within a particular member state. The GDPR focuses on the conditions and safeguards for transferring personal data to third countries.[267] Recent legislative developments, such as the European Health Data Space (EHDS)[268], further structure access to, and the secondary use of, health data across Member States by promoting interoperability and common governance mechanisms, without introducing general data-residency obligations. The EHDS aims to facilitate access, quality and re-use of health data for research and innovation, while channeling such uses through harmonized access frameworks rather than geographical data-localization requirements.[269] The GDPR, in addition, extends its reach by applying to data handled by EU-based controllers or processors, even if their data are physically located outside the Union, thereby strengthening the EU's ability to exercise regulatory authority over personal data.[270] For EU-based controllers, the primary legal consideration is therefore not where data must be stored, but rather how international transfers can be lawfully executed, typically through mechanisms such as adequacy decisions, EU-SCCs and TIAs.[271] Transfers to countries outside the EU are only permitted if the applicable transfer mechanism ensures a level of protection essentially equivalent to that required by EU law, as extensively discussed in Section 4.2. This approach reflects the EU's broader strategy to exercise regulatory influence and promote its data-protection standards beyond its territorial borders.[272]

---

[263] The GDPR aims to not only regulate the protection of personal data, but also the "free movement of such data" as per the official title of the Regulation.
[264] Ibid para. 155; *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 188.
[265] *McKibbin/Shabani*, The Journal of Law, Medicine & Ethics 2023, 301-302.
[266] *Gao*, Chinese J Int Law 2023, para. 74; *Chen*, US-China Law Review 2021, 264.
[267] See Article 44-49 GDPR.
[268] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, OJ L 2025/327, 05.03.2025.
[269] See European Health Data Space.
[270] *Chen*, US-China Law Review 2021, 264.
[271] Article 44-49 GDPR; see also *Hallinan*, Life Sciences, Society and Policy 2020.
[272] *Chen*, US-China Law Review 2021, 264.

At the same time, the EU's data governance instruments, such as the Data Governance Act[273] and EHDS[274], structure and condition international sharing of non-personal health and genetic data.

There is one EU framework that is regularly sparking discussions on data sovereignty requirements. The European Cybersecurity Certification Scheme for Cloud Services (EUCS), which is part of the EU Cybersecurity Act[275], is intended to establish a framework for standardized cybersecurity certification for cloud solutions in the Union.[276] The first draft of the European Cybersecurity Certification Scheme for Cloud Services (EUCS) published by ENISA in December 2020[277] included sovereignty requirements specifically for the highest level of cybersecurity standards (High+). The aim was to ensure that the cybersecurity level High+ could only be achieved if data are hosted in Europe.[278] The proposal has been highly debated.[279] In the subsequent draft from March 2024, data sovereignty requirements for High+ level security were omitted. A published final draft is, at present, not publicly available.[280]

4.6.2. China's localization regime and data sovereignty strategy

Several jurisdictions[281], including China, impose data localization requirements as part of broader cybersecurity and national security strategies. China's approach to data governance is distinctly different from the EU's fundamental rights model. It prioritizes national security and cyber sovereignty, embedding localization requirements in core statutes.[282]

---

[273] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 03.06.2022; Article 5 Data Governance Act empowers the Commission to adopt delegated acts establishing specific conditions for the international transfer of public sector data considered highly sensitive, such as many types of health and genetic data as identified by the Data Governance Act.

[274] See specifically Article 61 EHDS.

[275] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 07.06.2019.

[276] *Eckhardt/Hoffmann,* EU Cloud Certification at an Impasse, https://www.cep.eu/eu-topics/details/eu-cloud-certification-at-an-impasse.html (accessed 19.10.2025); ENISA, EUCS – Cloud Services Scheme, issued December 2020, https://certification.enisa.europa.eu/document/download/c14f76c8-99e8-4900-a2c2-a412fa3ab071_en?filename=EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf (accessed 01.02.2026); European Commission, EU Cloud Certification Scheme, https://ec.europa.eu/newsroom/cipr/items/713799/en, accessed 19.10.2025.

[277] *Eckhardt/Hoffmann,* EU Cloud Certification at an Impasse, https://www.cep.eu/eu-topics/details/eu-cloud-certification-at-an-impasse.html (accessed 19.10.2025); ENISA, EUCS – Cloud Services Scheme, 2020.

[278] European DIGITAL SME Alliance, Changes to the EU Cloud Services Cybersecurity Certification Scheme put EU citizens' data at risk: A Call for Digital Sovereignty, https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty (accessed 19.10.2025).

[279] Several stakeholders have issued opinions, such as the European Banking Federation (EBF, Joint Statement on EUCS, https://www.ebf.eu/wp-content/uploads/2023/11/Joint-Statement-on-EUCS.pdf (accessed 23.12.2025)), the European DIGITAL SME Alliance (European DIGITAL SME Alliance, Policy Paper, EU Certification Scheme for Cloud Services: An opportunity for Europe's Digital Sovereignty, https://www.digitalsme.eu/digital/uploads/Policy-Paper-EU-Certification-Scheme-for-Cloud-Services.pdf (accessed 23.12.2025)) and the Federation of German Industries (BDI) (BDI, European Cybersecurity Certification Scheme for Cloud Services (EUCS), https://english.bdi.eu/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs (accessed 23.12.2025)).

[280] *Eckhardt/Hoffmann,* EU Cloud Certification at an Impasse, https://www.cep.eu/eu-topics/details/eu-cloud-certification-at-an-impasse.html (accessed 19.10.2025).

[281] Others are Russia and Pakistan (see DLA Piper, Collection and Processing in Russia, https://www.dlapiperdataprotection.com/?t=collection-and-processing&c=RU#insight (accessed 01.02.2026); Global Network Initiative, Data localization: A Global Threat to Human Rights Online, https://globalnetworkinitiative.org/data-localization-a-global-threat-to-human-rights-online/ (accessed 23.12.2025)).

[282] *Chen*, US-China Law Review 2021, 261-273.

Article 37 CSL requires Critical Information Infrastructure Operators (CIIOs) to store personal data and Important Data generated or collected within Mainland China on local Chinese servers. Where it is necessary to transfer such information abroad, the CSL mandates a security assessment unless otherwise provided by law.[283] The PIPL reinforces those requirements for CIIOs and extends the localization obligations to entities processing large volumes of personal or sensitive data.[284] What constitutes processing at scale is defined by CAC implementing rules. Processing personal data of more than one million individuals, as well as the processing or transfer of sensitive personal data above thresholds specified by CAC rules, is considered processing at large scale.[285]

China's HGR regime imposes de facto localization requirements through the collaboration requirement as stipulated in Article 7, 21 and 24 HGR Regulation. This includes the requirement to provide full access and a backup to the Chinese partner.

In addition to HGR-specific rules, Chinese health sector regulations require that population health information (PHI) be stored on servers located within China. While these rules are primarily directed at medical institutions, they have practical implications for research collaborations, as clinical partners are often subject to these considerations. This reinforces the need for onshore data repositories and careful management of cross-border access rights.[286]

Further, the accumulation and preservation of Chinese HGR in Mainland China by foreign entities is effectively prohibited,[287] and strict guardrails on direct access to HGR by non-domestic researchers are in place.[288] These requirements function as a de facto localization mandate for both physical samples and digital data, regardless of whether the data transfer regime would otherwise permit cross-border movement.

Beyond localization mechanisms, China's HGR and biosecurity regime is explicitly strategic. As *McKibbin and Shabani* (2023) argue, Chinese policies treat genetic data as a national strategic resource, prioritizing national autonomy and national and economic security, alongside scientific aims.[289] In practice, this translates into sole national autonomy over HGR and government-overseen collaborations, with approvals, domestic storage and backups and security reviews acting as gatekeepers for international access.[290]

---

[283] Article 37 CSL; *Gao*, Chinese J Int Law 2023, para. 135-136.
[284] Article 40 PIPL.
[285] Article 4 Measures for the Security Assessment of Data Exports.
[286] *Wang/Gregg/Du*, Regulatory barriers to US–China collaboration for population health research, Cell Genomics 2022, 2-4.
[287] Article 7 HGR-Regulation restricts foreign entities, institutions and persons from collecting or preserving Chinas HGR within China and from providing China's HGR abroad.
[288] *Wang/Du*, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data, Perspectives in Law, Business and Innovation, Springer 2025, 192 f.
[289] *McKibbin/Shabani*, Journal of Law, Medicine & Ethics 2023, 301-302.
[290] Ibid, 302-304.

These developments entail several systemic consequences for international research collaboration and data governance. The increasing prioritization of national strategic interests in the regulation of genetic data places considerable strain on established principles of reciprocity and mutual benefit, for example by restricting data access for foreign partners and by introducing uncertainties regarding the long-term availability of shared datasets.[291]

McKibbin and Shabani further argue that those laws and strategies already have a chilling effect on cross-border scientific cooperations with Chinese partners. The authors state a case in which genetic data associated with an international publication was retracted at the request of the Chinese institution.[292] This example highlights the heightened uncertainty for researchers resulting from the discretionary and often not transparent nature of security review procedures.[293]

[291] Ibid, 307.
[292] *Cai et al.*, Retraction Note: 11,670 whole-genome sequences representative of the Han Chinese population from the CONVERGE project, Scientific Data 2020, 1.
[293] *McKibbin/Shabani*, Journal of Law, Medicine & Ethics 2023, 304 and 307.

5. Ethical and consent framework

Ethical considerations are a core aspect of biomedical research, particularly when human biospecimens and sensitive genetic and health data are utilized and when research includes vulnerable individuals. While research must create value for society to be justified, respect for human rights and fair treatment of research participants and communities remain non-negotiable.[294]

The Declaration of Helsinki (2024) confirms that research purposes "*can never take precedence over the rights and interests of individual research participants*".[295] However, as a non-binding ethical instrument, its impact depends on its translation into legal governance, Ethics Review Committees (ERC) decisions and local legislation, a critical factor when ethical principles intersect with GDPR and PIPL compliance.[296]

As EU and China follow fundamentally different regulatory philosophies, this creates complexity for cross-border research.[297] The Chapter 5 addresses the research question "*How can ethical principles, specifically informed consent and the protection of vulnerable populations, be operationalized in EU-China preclinical cancer research collaborations?*". It examines frameworks such as the EU Charter of Fundamental Rights of the European Union, CIOMS Guidelines, Declarations of Helsinki, Declaration of Taipei and the Belmont Report[298], focusing on informed consent, ethical review mechanisms and protection of vulnerable populations.

5.1. Ethical principles in biomedical research

Biomedical research implicates several fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (CFR)[299], including human dignity, the right to the integrity of the person, respect for private life and the protection of personal data.[300]

[294] CIMOS Guideline 1, 1.
[295] DoH 2024, para 7.
[296] *Bibbins-Domingo/Brubaker/Curfman*, Editor's Note: The 2024 Revision to the Declaration of Helsinki: Modern Ethics for Medical Research, Journal of the American Medical Association 2025, 30.
[297] See Article 28-30, 40, 60 and 63-67 PIPL, Article 7, 9 and 21-24 HGR Regulation, Article 14 and 33 MOST Implementing Rules and Article 36-38 CBL.
[298] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012; CIOMS, International Ethical Guidelines for Health-related Research Involving Humans, 2016; The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, The Belmont Report, Ethical Principles and Guidelines for the Protection of Human Subjects of Research, issued 18.04.1979, https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf (accessed 01.02.2026); World Medical Association, Declaration of Helsinki, 2024; World Medical Association, Declaration of Taipei, 2016.
[299] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012.
[300] Article 1, 3, 7, 8, 31 and 21 CFR.

Article 3 CFR explicitly requires informed consent and prohibits making profit from the human body. These principles bind EU institutions and apply to research under EU law, including any research funded by the EU, such as Horizon Europe projects.[301]

International ethical frameworks and guidelines, such as the CIOMS'[302] International Ethical Guidelines for Health-related Research Involving Humans[303] (CIOMS Guidelines), the WMA's Declaration of Helsinki[304] and Declaration of Taipei[305], the Principles of Biomedical Ethics by Beauchamp and Childress (first edition published in 1979; 8th edition published in 2019)[306] and the Belmont Report (1979)[307], further play a pivotal role in medical and genetic research.

The Belmont Report (1979) establishes three core principles: (i) Respect for persons, which includes voluntary participation and providing participants adequate information, especially for those with limited autonomy, (ii) beneficence, which obliges researchers to maximize benefit and minimize harm; and (iii) justice, which ensures fair distribution of research benefits and burdens so that no group is disproportionately exploited or excluded.[308] However, the Belmont Report offers little guidance for today's highly data-intensive biobanking operations and secondary use enabled by AI and lacks operational guidance. Those gaps are visible when Belmont's general consent guidance is compared with CIOMS specific rules for data and biospecimen collection, storage, secondary use and governance.[309]

The CIOMS Guidelines are designed to offer internationally recognized ethical principles and operational details on topics such as informed consent, privacy and data protection, community engagement and protection of vulnerable groups.[310] Principle 32 DoH explicitly addresses the acquisition, handling, storage and secondary use of biological materials and data and links to the DoT for governance.

Kurihara et al. (2024) argue that the DoH should more explicitly address dynamic consent, the sharing of patient-level datasets and include a stronger link to the DoT, specifically relevant for

---

[301] Article 51 CFR; Article 19 Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013; European Research Council, Ethics guidance, https://erc.europa.eu/manage-your-project/ethics-guidance (accessed 09.11.2025).
[302] Council for International Organizations of Medical Sciences (CIOMS).
[303] Established by the CIOMS in collaboration with the World Health Organization, first version issued in 1982, latest revision in 2016; see CIOMS Guidelines, p. viii-ix.
[304] WMA, Declaration of Helsinki, 2024.
[305] WMA, Declaration of Taipei, 2016.
[306] See *Beauchamp/Childress*, Principles of Biomedical Ethics, 8th ed (2019).
[307] See The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, The Belmont Report, 1979.
[308] Ibid, 6-10; *Nagai/Nakazawa/Akabayashi*, The creation of the Belmont Report and its effect on ethical principles: a historical study, Monash Bioethics Reviews 2022, 157-170.
[309] See The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, The Belmont Report, 1979, 6-8; CIOMS Guideline 11 and 12.
[310] Guideline 7 (Community Engagement), Guideline 9 (Individuals capable of giving informed consent), Guideline 10 (Modifications and waivers of informed consent); Guideline 11 (Collection, storage and use of biological materials and related data), Guideline 12 (Collection, storage and use of data in health-related research), Guideline 15 (Research involving vulnerable persons), Guideline 16 (Research involving adults incapable of giving informed consent), CIOMS Guidelines, 2016.

AI and the use of real-world data for secondary purposes.[311] The 2024 DoH revision improved the fairness principles but left gaps requiring interpretation by ethics committees on the mentioned aspects and complementary frameworks.[312]

The DoT establishes additional ethical principles and a governance layer for secondary use of data and specimens in biobanks and health databases.[313] The definition of Biological Material covers biospecimen of deceased persons, requiring prior consent for post-mortem research or next-of-kin authorization and creating a dual regime to GDPR which excludes post-mortem data from its scope. The DoT further addresses consent, transparency and ethics committees' approval and monitoring.[314]

Other important international standards for biomedical and genetic research covering ethical concerns are the NIH (National Institutes of Health, USA) "Seven Principles for Ethical Research"[315], the OECD "Recommendation of the Council on Human Biobanks and Genetic Research Databases" (2009)[316], the UNESCO "Universal Declaration on Bioethics and Human Rights" (2005)[317], "ICH E6 Good clinical practice - Scientific guideline" (first adopted in 1996, last revised in 2025)[318], "ISO Standards for Biobanking" (ISO 20387:2018)[319] and specifically relevant for AI driven analytics, the WHO "Guidance on Ethics & Governance of AI for Health" (2021)[320]. Although some of these frameworks were developed decades ago, they continue to shape modern research governance and retain relevance today.

When translating international ethical principles into operational practice for EU-China collaborations, some challenges emerge.

---

[311] *Kurihara et al.*, Declaration of Helsinki: ethical norm in pursuit of common global goals, frontiers in Medicine 2024, 1-2.
[312] WMA, Revised Declaration of Helsinki adopted by the global medical community, strengthening ethical standards in clinical research involving humans, https://www.wma.net/news-post/revised-declaration-of-helsinki-adopted-by-the-global-medical-community-strengthening-ethical-standards-in-clinical-research-involving-humans/ (accessed 04.01.2026).
[313] Article 3 DoT.
[314] Principle 1, 4, 8, 11-15 and 19 DoT; Recital 27 GDPR.
[315] National Institutes of Health, Guiding Principles for Ethical Research, https://www.nih.gov/health-information/nih-clinical-research-trials-you/guiding-principles-ethical-research (accessed 01.02.2026).
[316] See OECD, Recommendation of the Council on Human Biobanks and Genetic Research Databases, adopted 22.10.2009, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0375 (accessed 01.02.2026).
[317] See UNESCO, Universal Declaration on Bioethics and Human Rights, adopted 19.10.2005, https://www.unesco.org/en/legal-affairs/universal-declaration-bioethics-and-human-rights?hub=387 (accessed 01.02.2026).
[318] While the International Council for Harmonization's Good clinical practice guidelines are focusing on clinical trials, they include standards on consent and oversight also relevant for preclinical research (See European Medicines Agency, ICH E6 Good Clinical Practice – Scientific Guideline, issued 1996, last amended 2025, https://www.ema.europa.eu/en/ich-e6-good-clinical-practice-scientific-guideline (accessed 01.02.2026)).
[319] See International Organization for Standardization, ISO Standards for Biobanking, ISO 20387:2018, issued 2018, https://www.iso.org/standard/67888.html (accessed 01.02.2026).
[320] See World Health Organization, Ethics and governance of artificial intelligence for health, adopted 28.06.2021, https://www.who.int/publications/i/item/9789240029200 (accessed 01.02.2026).

First, the Declaration of Helsinki, as well as China's MOST Implementing Rules mandate independent ethics review in each jurisdiction.[321] While intended to safeguard research participants, this leads to duplications and extended timelines. Ethical principles cannot resolve these bureaucratic delays as they arise from legal rather than from ethical requirements.

Second, harmonizing secondary use and consent governance remains complex. The CIOMS Guidelines and the DoT endorse governed broad or dynamic consent for the reuse of data and biospecimens.[322] However, aligning these models with GDPR's Article 89 safeguards and China's PIPL and HGR requirements for purpose-specific consent and mandatory filings means that governance details, such as transparency measures, the scope of reuse and boundaries of consent withdrawal, must be defined already in the research protocol to remain compatible with both systems.[323]

Finally, the non-binding nature of ethical codes such as the Declaration of Helsinki and the Declaration of Taipei limits their enforceability. Compliance depends on whether and how those principles are embedded into ethics committee practice, joint oversight agreements and commitments and ministerial filings. The CIOMS Guidelines emphasize that research should generate social and scientific value that benefits society. However, if the ethical principles cannot be enforced, they remain merely theoretical and fail to translate into practice.[324]

Beyond questions of enforceability, the role of ethical frameworks must be understood through their legal status. Ethical guidelines do not create binding obligations and cannot override statutory requirements, administrative approvals or national security controls in neither the EU nor China. Their normative influence depends on the extent to which they are embedded in domestic law, mandated by ethics committees or operationalized through regulatory oversight.[325]

5.2. Ethical review systems

Ethical review is essential for protecting participants, yet in cross-border research it can become a bottleneck. In practice, however, many challenges in EU-China collaborations stem not from ethical conflicts per se, but rather from regulatory divergence and structurally different administrative oversight systems.

Frameworks such as the Declaration of Helsinki mandate independent review in each jurisdiction, but they do not provide mechanisms for resolving conflicting decisions or timelines. *Dove*

---

[321] Principle 23 DoH; Article 31 MOST Implementing Rules.
[322] CIOMS Guideline 11 and 12, 41-49; Principles 11-15 DoH.
[323] Article 31 MOST Implementing Rules.
[324] *Kurihara et al*., frontiers in Medicine 2024, 1-2; *Bibbins-Domingo/Brubaker/Curfman*, Journal of the American Medical Association 2025, 30.
[325] See Article 288 Treaty on the Functioning of the European Union, OJ C 115, 09.05.2008.

and Garattini (2018) emphasize that inconsistency, duplication and insufficient communication among ethics committees are among the most prominent challenges. As a common thread the authors have identified the challenge of trust building between IRBs, relying on reviews and decisions taken by each other.[326]

In the EU, ethical review is a cornerstone of biomedical research and should ensure compliance with legal and ethical standards. The system remains fragmented due to the lack of a single, harmonized system for ethical review. Instead, ethical oversight is governed by a combination of EU directives, national laws and international guidelines.[327] All genetic and biomedical research involving human participants must be reviewed and approved by an independent Research Ethics Committee (REC)[328]. These committees assess the scientific validity, risk-benefit ratio, informed consent process, data protection measures and the protection of vulnerable groups.[329] The Clinical Trials Regulation[330] introduced coordinated assessments for clinical trials but leaves the composition and procedures of RECs to national law.[331] GDPR adds additional complexity. While Article 89 GDPR permits research derogations, it does not harmonize ethics review standards, leaving ethics committees to interpret safeguards potentially inconsistently.[332] This potentially results in fragmented requirements, with variations in REC procedures and capacities across EU Member States. Such a fragmented approach may create challenges for multi-centered and cross-border research, particularly in collaborations with non-EU partners.

China's ethical governance of biomedical and life science research evolved significantly following global controversy surrounding the He Jiankui gene-editing case.[333] In 2018, the researcher used CRISPR technology[334] to edit the genomes of human embryos, resulting in the birth of genetically modified children, which was intensively debated in both the public and academia.[335] Following these debates, the "Measures for Ethical Review of Life Sciences and Medical Research involving Human Beings" (2023 Measures) have been issued.[336] The 2023 Measures broadened oversight to all research involving human participants, biospecimen and

---

[326] Principle 23 DoH.
[327] *Haimberger*, Datenschutz, 30 ff.; CIOMS, International Ethical Guidelines for Health-related Research Involving Humans, 2016, Guideline 23.
[328] Also known as Institutional Review Boards (IRB).
[329] CIOMS, Guideline 23; *Haimberger*, Datenschutz, 30 ff.
[330] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, 27.05.2014.
[331] Article 2, 4 and 7 Clinical Trial Regulations.
[332] *Staunton et al.,* frontiers in Genetics 2022, 2-3.
[333] See *Greely*, CRISPR'd babies: human germline genome editing in the 'He Jiankui affair', Journal of Law and the Biosciences 2019, 116.
[334] CRISPR stands for 'Clustered Regularly Interspaced Short Palindromic Repeats', See *Greely*, Journal of Law and the Biosciences 2019, 116.
[335] Ibid, 116.
[336] 2023 Measures for Ethical Review of Life Sciences and Medical Research Involving Human Beings (2023 Measures), issued 18.02.2023, original: https://www.nhc.gov.cn/qjjys/c100016/202302/6b6e447b3edc4338856c9a652a85f44b.shtml, English translation: https://www.lawinfochina.com/display.aspx?id=40963&lib=law (accessed 01.02.2026).

health related data, including research at universities and research institutes.[337] Institutions must establish independent ethics review committees with a diverse membership, regular training and clear conflict-of-interest management.[338] Reviews must address scientific and societal value, risk-benefit analysis, informed consent, confidentiality and protection of vulnerable groups.[339] China's approach integrates ethical oversight with national security objectives and data sovereignty objectives.[340] This potentially creates structural tension with international frameworks, that emphasize collaborative partnerships.[341] For cross-border research, ethics approval is required both from Chinese and foreign institutions. Exemptions apply for anonymized or publicly available data, for already existing human samples or cell-lines from biobanks that have been sourced in line with ethical standards.[342]

Joint ethical review models are increasingly proposed to address duplication and inefficiency.[343] These models aim to facilitate mutual recognition of ethical approvals, harmonize consent documentation and data protection standards and promote transparency, accountability and participant trust across jurisdictions.[344] Key recommendations include the development of shared ethical review protocols based on international guidelines. Joint Ethical Review would further include the establishment of clear procedures for cross-border consent, data sharing, the handling of data subject rights and the encouragement of ongoing dialogue between regulators, researchers and the participant communities.[345]

However, the practical implementation of joint ethical review remains challenging. While international guidelines provide a normative foundation for shared standards, they do not resolve the underlying legal and institutional differences between the EU and China. For example, the CIOMS Guidelines recommend collaborative partnership and capacity-building, but do not specify how to operationalize mutual recognition in the face of liability concerns.[346] The ethical review framework for EU-China research reflects both convergence and divergence. While both jurisdictions emphasize autonomy, transparency and data subject protection, their legal and institutional approaches differ significantly. Bridging these gaps requires not only legal harmonization but also operational collaboration through joint review models. While there is

---

[337] Article 2 2023 Measures.
[338] Article 5-10 2023 Measures; As per Article 13 2023 Measures, Ethics committees are subject to institutional and participant supervision, with mandatory registration, annual reporting and quality control systems.
[339] Article 17 2023 Measures; *Gang/Peng,* Biotechnology Law Report 2023, 152.
[340] See Article 8 MOST Implementing Rules; Article 53 CBL.
[341] CIOMS Guideline 8.
[342] Article 32 2023 Measures.
[343] See *Cavaleri et al.,* A roadmap for fostering timely regulatory and ethics approvals of international clinical trials in support of global health research systems, Lancet Global Health 2025, e769-e777; *Dove et al.,* Research Ethics. Ethics review for international data-intensive research, Science 2016, 1399-1400; *Dove/Garattini,* Expert perspectives on ethics review of international data-intensive research: Working towards mutual recognition, Research Ethics 2018, 1-25; *Rothstein et al*., Streamlining ethics review for international health research, Science 2022, 825-826.
[344] CIOMS, Guideline 23.
[345] CIOMS Guideline 24.
[346] CIOMS Guideline 8.

a growing movement toward harmonization, significant differences in legal culture, regulatory detail and enforcement remain.[347]

Mutual recognition of ethics reviews could reduce inefficiency and inconsistency, but diverging frameworks, liability concerns and institutional trust barriers make implementation challenging. Without enforceable mechanisms, joint ethical review risks remain aspirational rather than feasible. This process requires coordinated efforts, leadership and demonstrable value through improved communication, harmonized procedures, and operational planning.[348] The lack of legal mechanisms for recognizing foreign ethics committee review decisions in both the EU and China means that researchers must often navigate duplicative, time-consuming and sometimes inconsistent review processes.

5.3. Consent from an ethical perspective

International frameworks such as the Declaration of Helsinki, the Belmont Report and the CIOMS Guidelines emphasize that consent must be freely given, informed and comprehensible, supported by independent ethical review. Generally, consent should be documented and renewed in case of substantive changes in any aspects of the study. [349]

The EU permits broad and dynamic consent models. Ethically, broad consent, while offering flexibility for future research, raises questions about whether such consent fulfils the requirement of being informed when future uses of the data are unknown at the time of consent collection. [350]

Dynamic consent enhances transparency and control, but introduces new ethical challenges, e.g. when severely ill patients are repeatedly contacted for consent, raising questions about autonomy and proportionality in research governance.[351] Frequent requests for consent can further lead to consent fatigue, where participants approve without fully considering the implications. Additionally, reliance on digital platforms for exercising dynamic consent can raise concerns about accessibility and equity, specifically for individuals with limited technology literacy and resources.[352] These factors show that while dynamic consent mitigates some limitations of broad consent, it creates new ethical and practical dilemmas requiring careful governance.

---

[347] *Gang/Peng*, China Releases Document on Ethics Review of Life Sciences: Comments and Compliance Guideline, Biotechnology Law Report 2023, 153.
[348] *Gove/Garattini*, Research Ethics 2018, 14-25.
[349] CIOMS Guideline 9 and Guideline 10.
[350] Recital 32 GDPR; *Hallinan*, Life Sciences, Society and Policy 2020, 5–7; *Herbst*, Datenschutz und Datensicherheit 2016, 373.
[351] *Hänold,* Die Zuverlässigkeit eines "broad consent" in der medizinischen Forschung – a never ending story? ZD-Aktuell 2020, beck-online.beck.de (accessed 01.02.2026).
[352] *Prictor/Teare/Kaye*, Equitable Participation in Biobanks: The Risks and Benefits of a "Dynamic Consent" Approach, frontiers in Public Health 2018, 4.

Scholars debate the primacy of consent as a legal basis. *Hallinan* (2020) argues for explicit consent to uphold informational self-determination[353], while *Bord and Caruana* (2021) highlight that consent is often legally fragile and advocate for a broader application of Article 9(2)(j) GDPR in conjunction with Article 6(1)(e) GDPR for research in the public's interest. Also, explicit consent could be potentially ethically problematic in scientific contexts, for example if study participants depend on participating in a clinical trial to receive innovative treatment. This debate is critical for EU-China collaborations, where fragmented implementation of GDPR provisions create uncertainty for cross-border data exchange. The GDPR does not establish a strict hierarchy among the available legal bases for processing, leaving the choice of an appropriate legal to be determined on a case-by-case basis, which might be ethically complex in certain research contexts. [354]

China's legislators emphasize informed, purpose-specific consent, particularly for sensitive data such as genetic information.[355] Legislation mandates consent for any activity involving human genetic resources (HGR), including cross-border transfer. Consent must generally be documented in writing and, if this is not feasible, oral consent supported by documentation including audio/video records is an option. The informed consent must include detailed disclosures regarding the scope and method of data use, confidentiality measures, participant rights (including withdrawal, compensation and access to new information) and the handling of biospecimens. Where biological samples are involved, the form must also specify their type, quantity, intended use, storage conditions, potential for reuse or external provision and destruction protocols.[356]

The EU and China have distinct ethical approaches to consent. The differences create ethical and operational tensions in cross-border research, particularly for biobanking and secondary data use. Harmonizing consent documentation requires addressing language, cultural differences and divergent legal requirements.[357]

---

[353] *Hallinan* further supports this view by referencing Recital 33 GDPR, which endorses broad consent for scientific research, suggesting a legislative preference for consent where feasible (*Hallinan*, Life Sciences, Society and Policy 2020, 6).
[354] *Borg/Caruana*, Alternative Legal Bases for Processing Health Data for Scientific Research Purposes, Masaryk University Journal of Law and Technology 2024, 6-11, 20 and 21; *Hallinan*, Life Sciences, Society and Policy 2020, 6.
[355] The foundational principle of the PIPL, as stated in Article 1, is the protection of the rights and interests of individuals in relation to their personal information. In line with this objective, researchers engaging in data collection must ensure that participants are adequately informed of their rights prior to giving consent. The data subject rights, which are broadly aligned with international data protection standards, such as GDPR, include the ability to access and obtain copies of their personal data (Article 45 PIPL), to correct inaccuracies (Article 46 PIPL), to request deletion under certain conditions (Article 47 PIPL) and to transfer their data to other entities (Article 45 PIPL). Individuals also retain the right to be informed and to exercise autonomy over how their data is processed (Article 44 PIPL), including the right to withdraw consent at any time (Article 16 PIPL). When handling sensitive personal data, such as genetic data, the PIPL imposes heightened obligations on the Controller. According to Article 28 PIPL, such data may only be processed where there is a clearly defined purpose, demonstrable necessity and robust protective measures in place. Moreover, separate consents must be obtained for each category of sensitive data (Article 29 PIPL) and Controllers must explain both the necessity and potential impact of the processing to the data subjects (Article 30 PIPL).
[356] Article 9 HGR Regulations; Article 33 and 36 2023 Measures.
[357] *McKibbin/Shabani*, Journal of Law, Medicine & Ethics 2023, 301-304; *Staunton et al.*, frontiers in Genetics 2022, 5-8.

Preclinical studies and biobanking present consent challenges for secondary use. Re-contacting donors for each new purpose is often impractical, yet ethical integrity demands participant control over their biospecimens and data.[358] Ethical consent must include clear information about the limits of anonymization, the potential for data sharing and the boundaries of withdrawal rights.[359]

Drawing on international standards and the analysis in previous sections, ethically valid consent in EU-China preclinical research should meet several criteria. Consent materials must be accessible and understandable, considering language and cultural differences. Translation and community engagement are essential to ensure that participants genuinely understand their choices.[360] Robust governance, such as pseudonymization, data minimization and independent oversight, must complement consent models to enable ethically sound secondary use in preclinical research.

5.4. Secondary use of data and biospecimen

Secondary use is particularly relevant in the context of biobanking and large-scale data repositories, where samples and data may be reused for new scientific questions that could not have been anticipated at the time of initial consent.[361] A core challenge is the need to re-consent, particularly under Chinese law where purpose-specific consent for each new use case is mandated.[362] Re-contacting donors for secondary use is often highly impractical, particularly for pseudonymous samples and when re-identification would compromise privacy safeguards. In biobanks additional barriers include outdated contact information, high administrative costs and the sheer scale of patient cohorts that make re-contact efforts resource intensive. [363]

In contrast GDPR permits broad consent as already discussed in detail.[364] Equally pressing is the risk of re-identification, as genetic data and linked biospecimens remain inherently identifiable despite pseudonymization, making full anonymization unrealistic. Empirical studies and

[358] Ibid.
[359] Ibid.; see also: *Alser et al.* in *Garcia-Alfaro/Livraga/Roudier/Soriente* (eds.), Data Privacy Management, and Security Assurance (DPM 2015, QASA 2015), Lecture Notes in Computer Science, 237–244; *Marnau/Berrang/Humbert*, Datenschutz und Datensicherheit 2018, 4-6.
[360] The DoH, the DoT and the 2005 UNESCO Universal Declaration on Bioethics and Human Rights address the involvement of local communities via community consent, consultation and interest. The CIOMS Guidelines further encourage the engagement of communities and participants throughout the research life cycle (*Staunton et al.*, frontiers in Genetics 2022, 6-8; see also CIOMS Guideline 7).
[361] *Mathews et al.*, Secondary Use of Patient Tissue in Cancer Biobanks, The Oncologist 2019, 1577.
[362] Article 28 and 29 PIPL.
[363] See *Chen/Berkman/Hull*, Recontacting participants for expanded uses of existing samples and data: a case study, Genetics in Medicine 2017, 884-885; *Mathews et al.*, The Oncologist 2019, 1582-1583.
[364] Recital 33 GDPR.

regulatory commentary underscore that identifiability persists even after multiple de-identification steps, with linkage attacks across datasets posing additional risk.[365] International guidelines, most notably the CIOMS Guideline 12 and the Declaration of Taipei, require that such risks are mitigated through robust governance and transparency.[366]

Both EU and Chinese frameworks cover the need for ethics committee review, yet diverge on consent flexibility, creating operational complexity for cross-border research.[367]

5.5. Protection of vulnerable populations

The CIOMS Guideline 15 states that vulnerable individuals require special protection as they may have limited capacity to safeguard their own interests. However, they should not be excluded from health-related research unless there is a valid scientific justification for their exclusion.[368] This means that the consent process has to be adopted and additional safeguards and oversight are needed to prevent exploitation. Permission from a legally authorized representative must reflect the participants' preferences and values and if the participant later gains capacity, their consent must be obtained. For individuals not capable of consenting, the risks of a specific study must be minimized.[369]

Both, the GDPR and China's 2023 Measures emphasize the protection of vulnerable groups, such as persons with disabilities, children, pregnant women and the elderly. In the EU, GDPR and related ethical guidelines require specific safeguards for vulnerable populations, including adapted consent processes and additional ethical scrutiny.[370] National laws (e.g. Austrian FOG) may provide further detail. Yet practical challenges persist in ensuring meaningful protection. In China, the 2023 Measures mandate special protection for vulnerable groups but lack detailed guidance on implementation. Ethical review committees are responsible for assessing risk, ensuring appropriate consent and monitoring ongoing protection, but capacity and consistency vary across institutions.[371]

Finally, there is a risk that, in wanting to avoid any legal or ethical risk, research and ethics committees may exclude vulnerable groups from research altogether, thereby denying them the potential benefits of participating in scientific research. This highlights the need for balanced governance that combines strong safeguards with inclusive participation.[372]

---

[365] See *Marnau/Berrang/Humbert*, Datenschutz und Datensicherheit 2018, 83–85; S*habani/Marelli*, EMBO reports 2019, 2-5;
[366] DoH para. 32; CIOMS Guidelines 11 and 12; *Mathews et al.*, The Oncologist 2019, 1577-1578.
[367] *Gang/Peng*, Biotechnology Law Report 2023, 149-151.
[368] CIOMS Guideline 16, 61.
[369] CIOMS Guideline 16, 61-63.
[370] Article 8 GDPR; Recital 38, 51 and 75 GDPR; Article 17 2023 Measures; CIOMS Guideline 15.
[371] Article 17 2023 Measures; *Gang/Peng*, Biotechnology Law Report 2023, 152-153.
[372] CIOMS Guideline 15 and 16.

6. Practical challenges and compliance strategies in EU-China research collaborations

Preclinical cancer research collaborations between the EU and China offer unique scientific opportunities but also present complex legal, ethical and operational challenges. This is especially the case when genetic and health data as well as genetic materials are accessed by and shared among several research parties. To illustrate the practical compliance challenges in a tangible manner, the following section introduces a fictitious use case that maps the life cycle and data flows of a preclinical research collaboration between parties based in the EU and China. Building on this model scenario, the chapter develops a structured analysis of key frictions between the two regulatory systems and outlines compliance strategies derived directly from these conflicts.

6.1. Fictional use case: EU-China PDX research

In the fictional use case, an EU-based pharmaceutical company collaborates with a Chinese oncology institute to develop patient-derived xenograft (PDX) models from tumor samples collected in Mainland China. The cooperation aims at testing a novel compound developed by the pharmaceutical company with the goal of assessing its efficacy across genetically diverse tumor samples. The project requires the transfer and analysis of sensitive genetic and clinical health data, as well as biospecimens across jurisdictions.

In this use case, the Chinese institute is the controller for the collection and storage of human biospecimens in the institute's biobank, the creation of new PDX models and source sequencing, subject to HGR approvals[373] and PIPL requirements for any outbound data transfer[374]. The EU party is the controller for designing its compound testing, conducting joint analysis and managing any EU import of the resulting analytics data, subject to the GDPR, in particular Chapter V for transfers from the EU to China. The parties jointly conduct the study and analyze the data.

The fictional use case illustrates typical governance constellations, allocation of roles and regulatory conflicts that arise in cross-border EU-China research constellations. Its purpose is to enable a structured discussion of compliance challenges.

6.2. Core compliance challenges

The following sections address the core compliance challenges arising from the fictional use case and provide a structured assessment of the legal and operational frictions that shape cross-border EU-China research collaborations. Where relevant, each subsection includes a

[373] According to the HGR Regulation, the MOST Implementing Rules and the FAQ regarding Human Genetic Resource Management.
[374] Article 38 PIPL and CBDF Provisions.

brief description of what the identified risk means for the PDX collaboration described in Section 6.1.

6.2.1. Divergent legal frameworks

EU-China research collaborations must navigate fundamentally different legal frameworks, which differ in scope, definitions and regulatory philosophy.[375] These divergences generate substantive conflicts regarding permitted processing operations, transfer conditions, ethical review standards and allocation of regulatory responsibilities. In the PDX scenario, this divergence becomes visible because the EU partner must comply with Article 9 and Article 44 ff GDPR for the same analytics steps for which the Chinese partner must apply PIPL and HGR requirements, resulting in parallel compliance obligations.

In the context of the use case, the parties must ensure that the processing and transfer of sensitive data and biospecimens comply with the applicable requirements under GDPR, PIPL and sector-specific Chinese regulations. Particular attention must be given to the differing scopes of application (e.g. certain biospecimens such as plasma or CDX models may fall outside the HGR regime).[376] Clear allocation of roles and responsibilities, as well as continuous monitoring of evolving Chinese and EU requirements, is essential to avoid regulatory gaps and inconsistent compliance approaches.

6.2.2. Divergent consent models and ethical requirements

A major source of complexity lies in divergent consent models and ethical requirements. GDPR allows for broad or dynamic consent for scientific research, offering some degree of flexibility for secondary use. Where permitted by Member State law, GDPR recognizes scientific research as a legal ground for processing special category data (Article 9(2)(j) GDPR in conjunction with Article 89 GDPR). In contrast, China's PIPL mandates purpose-specific consent and separate approvals for sensitive data and cross-border transfers, with no general research exemption. This creates constraints for long-term or evolving research projects, as changes in scope or purpose frequently trigger a renewed consent requirement under PIPL.[377] Further, both jurisdictions require independent ethical review, which may result in duplication, delays and inconsistent requirements in cross-border projects.

In the context of the use case, these differences mean that consent forms and ethical approvals must be carefully designed to satisfy both EU and Chinese requirements, particularly regarding

---

[375] Compare Article 1 (2) GDPR and Article 1 DSL; See *Creemers*, China's emerging data protection framework, Journal of Cybersecurity 2022, 1-2.
[376] See Q&A on Issues Related to the Management of Human Genetic Resources (Part II) and Questions IV.1, IV.2 and IV.3. FAQ regarding Human Genetic Resource Management.
[377] See EDPB Recommendation 05/2020; Recital 33 GDPR; Article 13 and 28-30 PIPL; *Li/Cong/Liu*, Science 2022, 714-715; *Staunton et al.*, frontiers in Genetics 2022, 7-8.

secondary use and cross-border sharing. This becomes relevant when EU-driven analytics can rely on broad or dynamic consent for secondary use, whereas the Chinese partner must initiate a renewed PIPL-compliant consent process if the scope of the analytics changes.

To manage these divergences in a PDX collaboration, the following recommendations can be delivered:

- Develop a harmonized consent framework, combining a layered information sheet (EU) with explicit, purpose-specific consent elements (China). Such harmonization enhances consistency but cannot replace re-consent mandated by PIPL.
- Ensure clear and consistent information on data reuse, cross-border transfers and withdrawal rights, reflecting both GDPR and PIPL requirements.
- Plan a structured re-consent process for China whenever the research purposes, scope or data use changes in a way that triggers PIPL or HGR obligations.
- Assess whether broad or dynamic consent can be used, or whether processing of data collected in the EU can be based on Article 9(2)(j) GDPR in conjunction with Article 89 GDPR, where Member State laws provide an appropriate legal basis and safeguards.
- Prepare bilingual, harmonized ethical review documentation to minimize discrepancies across review bodies.
- Coordinate parallel ethics review procedures in the EU and China to reduce administrative duplication and mitigate unnecessary delays.

6.2.3. Localization requirements and sector-specific controls

Despite recent reforms[378], research collaborations involving Chinese HGR and sensitive data face strict localization and sector-specific obligations under Chinese law. These obligations apply before any outbound transfer is considered and primarily govern domestic storage, onshore processing and regulatory approvals inside China.

Under the CSL and PIPL, localization requirements typically necessitate that certain categories of personal information and "Important Data" be stored and processed physically within Mainland China. This may require local infrastructure or partnerships with Chinese cloud providers. China's localization regime is anchored in the CSL, which obliges CIIOs to store personal information and Important Data domestically. The PIPL and its implementing rules further introduce volume-based triggers for outbound data transfers, defined through thresholds and procedural requirements in CAC regulations.[379]

[378] Such as the CBDF Provisions and the CAC's Q&A on Data Export Security Management Policies.
[379] Article 37 CSL; Article 40 PIPL; Measures for the Security Assessment of Data Exports.

Even remote access by foreign researchers to data stored in Mainland China is treated as a cross-border transfer, triggering filings and security assessments under CAC rules.[380] Any export of HGR materials or associated information requires prior approval or record filing with the NHC. Collaborations must also ensure domestic access and backups for Chinese partners throughout the project lifecycle.[381]

Additionally, health sector rules require Population Health Information (PHI) to be stored locally in China. This is applicable primarily for medical institutions and therefore indirectly applicable to research projects with clinical partners.[382] In practice, this necessitates onshore storage for PHI and careful management of role-based access, even where data are not formally classified as HGR.

Applied to the PDX scenario, the sequencing data generated in China must remain stored and analyzed onshore, restricting the EU partner to strictly necessary remote sessions, each of which qualifies as a cross-border transfer requiring additional filings.

To address these localization and sector-specific constraints, the following measures are recommended:

- Segment data flows and environments to separate HGR/PHI/sensitive personal information from other research data, ensuring that only data legally subject to localization strictly remain onshore.
- Use onshore compute and analysis in China where required by law and restrict remote access to strictly necessary, role-based sessions. Treat any remote access as a cross-border transfer for compliance purposes.
- Maintain legally required backup copies and continuous domestic access for the Chinese partner, in line with NHC/HGR access obligations.
- Plan NHC filings/approvals early, mapping HGR scope, roles and repositories to avoid delays or ex post regulations.
- Implement a standing regulatory monitoring tied to localization triggers and sectoral thresholds, ensuring ongoing compliance with evolving Chinese requirements.

6.2.4. (Foreign) collaboration requirements and sector-specific restrictions

When personal data and HGR materials are processed in collaboration, particularly when this collaboration spans across borders, it is subject to specific collaboration requirements. Where GDPR applies, a Joint Controller Relationship must be contractually established. In parallel,

[380] Question 5 Q&A on Data Outbound Security Management Policy.
[381] Article 7, 21, 24, 27 and 28 HGR Regulations; Article 37 MOST Implementing Rules.
[382] *Wang/Gregg/Du*, Cell Genomics 2022, 2-4.

Chinese law imposes mandatory domestic-partner and approval requirements for any foreign involvement in projects using Chinese HGR. Together, these regimes create structural compliance tension, especially regarding allocation of responsibilities, access rights and approval workflows.

6.2.4.1. Joint controller relationship

In multi-party research collaborations, joint controllership typically arises in several aspects of the project. Examples include when the research protocol is co-designed (e.g. selection of endpoints, animal models and sequencing methodology), the parties jointly decide on the data model (e.g. identifiers, pseudonymization keys and access roles) or establish shared analysis environments.[383] This constellation arises directly in the PDX use case, as both parties jointly determine endpoints, sequencing steps and analysis logic.

Given the GDPR's territorial scope, its obligations may extend to a Chinese research partner when the processing is linked to the activities of an EU entity – in this use case, the EU-based pharmaceutical company. A JCA may therefore be required even if one partner is located outside the EEA.[384] A Joint Controller Agreement does not replace Chapter V GDPR requirements. It applies in addition.

Under Article 26(1) GDPR, joint controllers must clearly and transparently set out how they allocate their respective duties for ensuring compliance, in particular with respect to Article 13 and 14 GDPR information obligations and the handling of data subject rights stipulated under Article 15-22 GDPR. The fundamental aspects of the JCA must be made transparent to data subjects.[385] The JCA should therefore (i) specify which party provides privacy notices to data subjects, (ii) identify a contact point for data subjects to exercise their rights and (iii) set internal timelines and evidence standards for responding to data subject requests.

Additionally, joint controllers must ensure appropriate technical and organizational measures (Article 32 GDPR), define responsibility for personal data breach detection, notification and communication (Article 33 and 34 GDPR) and agree on DPIA responsibilities (Article 35 GDPR).[386] Where special-category data are processed, the JCA should identify the relied-upon Article 9 GDPR legal basis for each processing operation (e.g. Article 9(2)(a), (g) or (j) GDPR in conjunction with Article 89 GDPR safeguards) and specify the concrete safeguards applied. The agreement must further address records of processing activities (Article 30 GDPR), retention schedules, logging/audit and the cooperation duties between the joint controllers including

[383] See for example related to in vivo preclinical research study design: *Moctezuma-Ramirez et al.,* Designing an In Vivo Preclinical Research Study, Surgeries 2023, 544-555; EDPB, Guidelines 07/2020, 2021, 22.
[384] Article 3(1) and (2) GDPR; Article 44–49 GDPR; EDPB Guidelines 3/2018, 2019, 4–5, 9, 13.
[385] Article 26(1) and (2) GDPR, Article 13-22 GDPR.
[386] Article 32–35 GDPR.

onward transfers.[387] While Article 26 GDPR does not mandate a specific form, a written agreement is best practice for accountability purposes and to make its essential terms accessible to the data subjects.

As already stated, a JCA is not a transfer tool. If personal data are disclosed from the EEA to a recipient in a third country, Chapter V GDPR applies. In the absence of an adequacy decision for China, joint controllers must implement appropriate safeguards under Article 46 GDPR, in practice EU-SCCs and conduct a TIA with supplementary measures where needed.[388]

The JCA should therefore coexist with the selected EU-SCC module matching the factual roles of the parties for the data flow in question as well as the TIA and its technical/organizational supplements (e.g. encryption at rest/in transit, split-key or controlled-compute access, strict role-based access controls), as they govern different aspects.[389]

On the Chinese side, the JCA cannot replace or dilute sector-specific obligations under the HGR Regulations and Biosecurity Law. The JCA should acknowledge the parallel tracks, specifically assigning responsibility for Chinese approvals and filings and reflect Chinese backup and access duties for the domestic partner where applicable.[390]

6.2.4.2. Chinese sectoral collaboration requirements

Chinese law imposes strict collaboration requirements on foreign entities processing Chinese HGR. Foreign organizations are prohibited from independently utilizing Chinese HGR. Instead, they must partner with a domestic institution, jointly apply for approval with the NHC and grant the Chinese party full access (including a backup) to any data processed and generated during the course of the research collaboration.[391] The NHC plays a central role in supervising compliance, requiring joint submissions[392] and ensuring that Chinese parties retain full access to research data and backups throughout the project lifecycle[393].

Applied to the use case, the EU-based pharmaceutical company cannot independently collect or analyze Chinese patient-derived tumor samples. It must formally partner with the Chinese institute, and both must jointly submit the research protocol, ethics approvals and the cooper-

[387] Article 30 GDPR.
[388] Article 46(2)(c) GDPR; CJEU C-311/18, ECLI:EU:C:2020:559, Schrems II; see also EDPB, Recommendations 01/2020 Annex 2.
[389] Article 46(1) GDPR; EDPB, Recommendations 01/2020.
[390] Article 21-24 HGR Regulation; Article 14 MOST Implementing Rules (continuous access/backup).
[391] Article 14 and 33 MOST Implementing Rules.
[392] Article 33 MOST Implementing Rules.
[393] Article 14 MOST Implementing Rules.

ation agreement to the NHC for approval before any collection, analysis or transfer of PDX models or analytics data can occur. All data and materials generated from Chinese HGR must be fully accessible to the Chinese institute and a backup copy must be provided.[394]

These requirements again highlight the necessity of early planning and negotiation with the Chinese partner. Additionally, the NHC application with a clear HGR scope must be prepared early on. To demonstrate compliance, any filing or approvals should be properly documented. Lastly, it must be ensured that the backup is provided to the Chinese partner. Contractual arrangements managing data access and, importantly, intellectual property are essential.

6.2.4.3. Summary of practical measures and strategies

To address sector-specific and foreign collaboration requirements, the following strategies are recommended:

- Establish a clear and detailed Joint Controller Agreement (JCA) that allocates compliance responsibilities, data subject rights and technical and organizational measures between EU and Chinese partners.
- Ensure the JCA's essence is made available to data subjects, e.g. as part of a privacy notice or by publishing the contents on a publicly available website.
- Conduct a granular analysis of the roles for each phase of the research project and document responsibilities for data protection, data breach notification and conducting a Data Protection Impact Assessment (DPIA), e.g., in the JCA.
- Ensure all foreign collaborations involving HGR comply with Chinese requirements for domestic collaborations, including access and backup obligations under the HGR Regulations and the Biosecurity Law.
- Clarify whether statutory exemptions under the HGR framework apply and document the justification.
- Maintain ongoing documentation to demonstrate compliance with both regimes.
- Engage in early planning and negotiation to anticipate and address sector-specific restrictions and approval timelines.

6.2.5. Cross-border data transfer mechanisms

Cross-border data transfer mechanisms present another challenge. China is not recognized as providing an adequate level of data protection under GDPR, requiring the use of Standard Contractual Clauses or other safeguards, mandatory Transfer Impact Assessment and supplementary measures for lawful transfers. Cross-border transfers from China abroad involving genetic

[394] Questions II.2 and II. 5 FAQ regarding Human Genetic Resource Management; Article 21 and 22 HGR Regulations; Article 31 and 33 MOST Implementing Rules; Section II, Questions 2 and 5.

data or PDX models are subject to both general CBDT mechanisms and HGR approvals, with thresholds for CAC security assessments.[395] In the fictional use case, these requirements govern both the initial transfer of EU generated data to the Chinese institute for validation and the subsequent return of HGR-derived analytics data to the EU partner, each triggering distinct approval and assessment steps.

Following the HGR approval/security review, the data exporter must comply with cross-border data transfer mechanisms specified via the CBDF Provisions. These Provisions introduce clearer thresholds and simplified exemptions.[396] The specific thresholds as well as transfer mechanisms are displayed in Figure 2.

The export of PDX models, genetic sequencing data or remote access to such data typically requires prior NHC approval or security assessment before any outbound transfer can take place. In addition, genetic sequencing data typically qualifies as sensitive personal information, so even moderate-scale datasets may trigger a CAC security-assessment under the CBDF framework.[397]

For the use case discussed in this chapter, genetic analytics data and health data are initially transferred from the EU to China, where the Chinese research institute validates the data prior to the conduct of the study. Subsequently, the Chinese party establishes PDX models utilizing HGR obtained in China. For the purpose of this use case, research conducted on these models is considered to take place under a joint controller constellation. Finally, analytics data are transferred back from Mainland China to the EU party.

6.2.5.1. EU to China data transfer: Transfer Impact Assessment (TIA) and supplementary measures

In the described use case, the EU party aims to transferring genetic analytics and health data to the Chinese party for validation. China does not have an adequacy decision under Article 45 GDPR. Therefore, any transfer of personal data from the EEA to China must rely on appropriate safeguards under Article 46 (see Chapter 4). Before any data is transferred based on Article 46(1) GDPR, a Transfer Impact Assessment (TIA) is obligatory.[398] A high-level step-by-step TIA

[395] Article 37-38 MOST Implementing Rules.
[396] See CBDF Provisions.
[397] Article 27-28 HGR Regulations; Article 36-37 MOST Implementing Rules; Question 5 Q&A on Data Outbound Security Management Policy.
[398] The aim of the TIA is to identify whether SCCs alone are sufficient or whether additional TOMs are required in order to ensure that the level of (data) protection in the recipient country is of equivalent level to the EU (See Court of Justice of the European Union Press Release No 91/20, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf, accessed 08.12.2025); The SCCs require that parties must warrant they have "no reason to believe that the laws and practices applicable to the data importer are not in line with these requirements." (Recital 19 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199, 07.06.2021).

for this use case is provided in Appendix 2. This section summarizes the key legal considerations relevant to the TIA. For the PDX use case, the initial analytics data cannot be shared unless the TIA concludes that effective supplementary measures achieve essentially equivalent protection for genetic data.

Whether the SCCs alone are effective in light of Chinese law and legal practice remains contested. The EDPB guidance requires that a TIA assesses the recipient country's legislation and practical access risk, including potential surveillance by authorities.[399] For China, this includes outbound data transfer rules, exemptions and real-world enforcement practices.

While encryption and pseudonymization align with EDPB guidance and are in theory highly effective[400], genetic data still poses a high re-identification risk. Additionally, joint analysis often requires raw data, making full anonymization highly impractical. While data minimization as well as audit trails are strictly necessary, their impact on systematic state access is insufficient. SCC clauses prohibiting onward transfers or requiring suspension are unlikely to be enforceable under Chinese jurisdiction. Even with robust safeguards in place, the risk of access by Chinese Authorities remains high for genetic data.[401]

EDPB guidance and Schrems II ruling[402] require suspension or avoidance of transfers where supplementary measures cannot ensure essential equivalence.[403] Thus, for this use case the transfer would only be lawful if effective anonymization can be achieved. Therefore, it would be advisable for the EU company to either conduct the analytics themselves or by a contractor in the EU or in a country where the TIA outcome would be positive.

If no personal data are transferred from the EU to China, but the Chinese party processes personal data and samples exclusively on behalf of the EU party, a Data Processing Agreement in accordance with Article 28 GDPR is still required.[404]

If both parties jointly determine the purposes of data processing (e.g. joint protocol design and shared research outcomes), a Joint Controller Agreement under Article 26 GDPR is mandated,

[399] EDPB, Recommendations 01/2020, 2021, para. 29-31; EU Exporters must spot supplementary measures or suspend/terminate/avoid the transfer in case the exporter cannot ensure an adequate level of personal data protection. (See EDPB, Recommendations 01/2020, 2021, 4).
[400] EDPB, Recommendations 01/2020, 2021, Annex 2; TeleTrust/ENISA, Guideline "State of the art" in IT security, Technical and organizational measures, adopted in 2025, https://www.teletrust.de/fileadmin/user_upload/2025-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf (accessed 01.02.2026).
[401] Article 28 CBL.
[402] CJEU C-311/18, ECLI:EU:C:2020:559, Schrems II.
[403] Step 5 and 6 include the deployment of the supplementary measures before the transfer takes place if those are deemed effective, including proper documentation and regular reassessment of the effectiveness (Step 5), as well as the monitoring and reassessment of the transfer (Step 6). As the regulatory environment in China is rather dynamic, requiring monitoring of legislative changes and potential adaptation of the TIA and supplementary measures required (See EDPB Recommendations 01/2020, 23-25).
[404] Article 28 GDPR.

independently of any data transfers and in addition to the SCCs. As clarified in Section 6.6.1., joint controllership under Article 26 GDPR does not replace Chapter V GDPR requirements.

6.2.5.2. China to EU data transfer: Sector-specific and general data transfer requirements

Transfers from China abroad involving PDX models or genetic sequence data require assessing two compliance processes: general cross-border data transfer mechanisms under the PIPL, DSL and CAC rules as well as sector-specific approvals.[405]

In the use case described in Section 6.1, this directly affects the planned transfer of sequencing-derived analytic data from China to the EU, which requires NHC approval or filing and – depending on the specific data type and volume – may also trigger a CAC security assessment.

Therefore, it is advisable to first identify the type of data intended for transfer. In case of HGR data, the HGR Regulations impose specific transfer restrictions. Also, personal data, Important Data or Core Data are handled differently under PIPL, the DSL and CSL.[406] The CBDF Provisions and Free-Trade Zone negative lists further allow certain data to be exported with fewer formalities.

It is also advisable to segment data flows and separate HGR and sensitive data from other research data so that only data subject to stricter controls are treated accordingly. Where HGR is involved, the sharing scenario (open access vs. authorized collaboration) determines the applicable filings.

In case of open access, the Chinese party must file with the NHC and provide a backup copy together with a demonstration of lawful basis, necessity and a risk self-evaluation. Data can also be shared as part of an authorized research collaboration and require no further filing if the collaboration has been authorized and the parties comply with all collaboration specific requirements. The NHC may additionally require a security assessment if national security could be affected, for example where HGR from vital genetic families, samples from sensitive regions or large-scale exome/genome sequencing (≥500 cases) are involved. As the NHC may identify further scenarios for which a security assessment is needed, there is uncertainty regarding when such an assessment is required and how it will be evaluated. Where HGR quali-

[405] *Chen/Li*, Is cross-border transfer of China's human genetic data an impossible mission? Human Genetics 2025, 3-4.
[406] For the definition of Important Data see the Appendix G of Data Security Technology – Rules for Data Classification and Grading (GB/T 43697-2024).

fies as Important Data under Chinese law, a parallel CAC security assessment may also be triggered in accordance with the Provisions on Promoting and Regulating the Cross-Border Flow of Data.[407]

Data can only be transferred out of Mainland China if the parties choose and comply with one of the four legal transfer mechanisms (Article 38 PIPL):

- Security Assessment by CAC (mandatory for CIIOs, Important Data/Core Data or large volumes of personal data or sensitive data)
- Standard Contracts (for non-CIIOs and below volume thresholds)
- Certification by accredited institutions or
- other legal basis as provided by law or the CAC (e.g. FTZ Negative List exemptions or CBDF Provisions).

It is therefore required to first check the thresholds and requirements in order to identify the proper transfer requirements. Segmenting data transfers to avoid thresholds is prohibited.

It should be noted that transfers under the Standard Contract or Certifications require a Personal Information Protection Impact Assessment (PIPIA) to be completed and filed with the CAC. In case data are transferred based on the Standard Contract, the contract and the PIPIA must be filed within 10 working days after signing. In case the processing changes substantially, a reassessment is required.[408] Any outbound transfer additionally requires purpose-specific consent.

Given approval uncertainties, exporting only essential data or conducting on-site analysis in China may be advisable to avoid triggering CBDT processes. Accordingly, the PDX scenario may need to rely on local analytics performed in China with only aggregated outputs exported.

6.2.5.3. Compliance strategies

To address the challenges of cross-border data transfers between the EU and China, the following strategies are recommended:

- Use Standard Contractual Clauses (SCC) and conduct a mandatory Transfer Impact Assessment (TIA) for all transfers from the EU to China. Ensure that the legal, regulatory and enforcement contexts in China are fully considered in the assessment.

[407] Article 36 and 37 MOST Implementing Rules; Article 7 of the Provisions on Promoting and Regulating the Cross-Border Flow of Data.
[408] Article 55 PIPL, Article 7, 8, 11 and 14 SC Measures.

- Prioritize processing of human biospecimens and special-category data within the EU where feasible. Where transfers are indispensable, limit exports to the minimum necessary data and document necessity and proportionality in the TIA.
- Implement supplementary technical and organizational measures, such as strong encryption (with keys held in the EU), pseudonymization at source, data minimization and strict access controls.
- If supplementary measures cannot ensure an essentially equivalent level of protection, suspend or avoid the transfer in line with EDPB guidance and the Schrems II ruling.
- Ensure that China-EU transfers comply with all applicable HGR and sector-specific requirements, including completing NHC approvals and CAC filings where required and maintain comprehensive documentation to record compliance.
- Explicitly address CAC security review triggers (e.g. vital genetic families, sensitive regions, exome/genome sequencing of more than 500 cases) and prepare for NHC or CAC security assessment where applicable.
- Limit data transfers to what is strictly necessary for specific research purposes and consider on-site analysis or export of aggregated/anonymized data where transfers are not feasible or lawful.
- Document all transfer mechanisms, approvals, contracts (including SCCs and TIAs).
- Regularly review and update compliance strategies in response to changes in Chinese and EU law and document all risk assessments and decisions, ensuring that any changes are reflected in the TIA, PIPIA and associated contractual safeguards.

6.2.6. Technical challenges and administrative burdens

In practice, data and samples are pseudonymized multiple times. First, when human biospecimens and associated data are obtained at the hospital and shared with the biobank. The biobank typically assigns its own key to the samples and data. Repeated pseudonymization of samples and data can be performed by a data trustee, who is contractually obligated to confidentiality. Whenever the data and samples are shared with a third party, they should be pseudonymized again, resulting in no individual party holding all keys. This multi-stage pseudonymization structure mitigates risks under both regimes. It reduces re-identification risks and supports necessity and minimization principles.[409]

By ensuring that no single party holds all the keys and by contractually ensuring the separation of identifiers, the risk of unauthorized re-identification is minimized, even in the event of a (data) breach. In the PDX use case, pseudonymization should occur at several stages as data

[409] *Herbst*, Datenschutz und Daten-sicherheit 2016, 375.

move from the hospital to the biobank, to the sequencing institution and finally to the collaboration partners. The keys are separated to ensure that neither the EU nor the Chinese partner can independently re-identify the donors.

The GDPR offers a robust framework for safeguarding data subject rights while accommodating the realities of scientific research by allowing targeted derogations under Article 89 GDPR when combined with proportionate safeguards. However, the fragmented implementation of key provisions, especially those concerning research exemptions and safeguards, across Member States introduces significant legal uncertainty. This fragmentation results not only from divergent Member State laws but also from heterogeneous interpretation by ethics committees and supervisory authorities, including divergent views on what constitutes appropriate safeguards.

For EU-China collaborations, these differences have significant operational consequences. While EU partners may leverage broad consent and research exceptions to facilitate data sharing and secondary use, Chinese partners must navigate a more rigid, approval-driven system that can impede multi-phase or cross-project research. The administrative burden of re-consenting, dual ethical approvals and continuous regulatory filings is particularly significant in joint biobanking or PDX workflows. These burdens interact with localization and sectoral requirements (see Section 6.5. and 6.6.), increasing coordination costs and documentation demand across jurisdictions.

While the GDPR provides a comprehensive framework, its effectiveness in cross-border research settings depends on the clarity of legal bases, the harmonization of safeguards, and the operationalization of compliance mechanisms. The security management mechanisms of HGR and biological resources stipulated in Chapter IV CBL are designed to align with China's broader data sovereignty agenda and are particularly relevant in cross-border research contexts, where foreign institutions must navigate multi-tiered approval processes and demonstrate adherence to Chinese ethical and security standards. This regulatory model introduces complexity for international research teams and underscores the need for harmonized compliance strategies.

To address technical and administrative challenges, the following strategies may be considered:

– Implement multi-stage pseudonymization at each transfer point, combined with contractual separation of keys and identifiers. Recognize that pseudonymization (particularly for genetic data) does not equal anonymization and must be complemented by additional safeguards.

- Ensure contractual separation of identifiers and keys (e.g. via a data-trustee model), prohibiting any single party from holding all re-identification elements.
- Apply robust encryption (in transit and at rest with EU-held keys), strict access controls, logging and data minimization, considering the likelihood of identifiability of genetic data.
- Map roles and processing chains for any steps of the research project (controller/processor/joint controller/third party) and align accountability and notification and escalation flows.
- Document safeguards specific to genetic data (e.g. pseudonymization, secure computing, access control), as those are a critical element in Article 82 GDPR liability assessments.
- Maintain comprehensive, up-to-date documentation (e.g. safeguards, TIA, PIPIA, DPIA, contracts, ethics committees' decisions, meeting minutes).
- Continuously update the TIA/PIPIA as legal, factual and technical conditions develop. Reflect any changes in SCCs, Joint Controller Agreements and related instruments.
- Operationalize governance with structured registers, checklists and tools for project management that track obligations, deadlines and documentation requirements.
- Plan periodic monitoring of legal and technical developments to proactively identify compliance risks and gaps.
- Embed technical and organizational measures (access controls, logging, secure environments) contractually in JCAs and SCCs, ensuring consistency with the role map and transfer records.
- Ensure robust documentation of the DPIA (Article 35 GDPR), ethical approvals and meeting minutes. Documentation is essential to accountability and may mitigate enforcement exposure.

6.2.7. Data subject rights and transparency

Upholding data subject rights and ensuring transparency and the possibility to withdraw consent are also challenging, especially for secondary use and biobank research.

In the context of biobank research, this flexibility has led to a fragmented landscape. As Staunton notes, while the GDPR formally grants data subjects rights, the actual enforceability of these rights is often limited in practice.[410] For instance, if data are not collected directly from the data subject, the right to information under Article 14 GDPR may be waived on grounds of disproportionate effort or if providing the information would seriously impair the research purpose.[411] This has direct implications for the exercise of other data subject rights, which can only

[410] *Staunton*, Individual Rights in Biobank Research Under the GDPR, in: *Slokenberga et al.* (ed.), GDPR and Biobanking, Law, Governance and Technology, 2021, 100-101.
[411] Article 14(5) GDPR.

be exercised when the data subject is aware that their data are being processed.[412] Moreover, the right to erasure is significantly constrained in research contexts. Article 17(3)(d) GDPR explicitly exempts controllers from complying with erasure requests if doing so would impair the research, provided that appropriate safeguards under Article 89 (1) GDPR are in place. This means that once data are incorporated into a biobank, the data subject may lose meaningful control over their future use.[413] The structural limitations are highlighted in EU-China collaborations, where divergent consent models (see Section 6.4.) and multi-tiered approval processes (see Section 6.6.) increase the complexity of offering effective rights mechanisms. In particular, PIPL's purpose-specific consent model and Chinese ethical review requirements can create operational misalignment with GDPR's research framework, which permits the use of broad consent. In the fictive PDX collaboration scenario, this results in parallel obligations for handling of data subject rights. The EU partner must respond to GDPR access, information or erasure requests even where primary data are held in China, while the Chinese partner must manage PIPL-compliant consent withdrawals and scope changes for data processing under their control.

To address challenges while upholding data subject rights and ensuring transparency, the following strategies are recommended for the use case:

- Provide layered transparent privacy notices and consent forms that reflect both GDPR and PIPL expectations. Ensure that information about processing, cross-border sharing and withdrawal rights is accessible, clear and tailored to the context.
- Clearly document and justify any derogations from data subject rights: Where research exemptions apply (e.g. limitations on the right to information or erasure under GDPR), maintain a record explaining the legal and ethical grounds for these limitations.
- Establish practical mechanisms for managing data subject rights, including procedures for withdrawal of consent (if applicable) and for handling access and information requests, and ensure that these mechanisms are aligned with the role allocation defined in Section 6.6.

6.2.8. Enforcement and liability risks

Finally, both EU and Chinese laws provide for significant administrative fines, including personal liability and, in severe cases, criminal sanctions for non-compliance. Differences in enforcement practice and risk of regulatory intervention or project suspension add to the compliance risk. For EU-China collaborations, common risks include missed filings or approvals,

[412] *Staunton*, in: *Slokenberga et al.* (eds.), GDPR and Biobanking, Law, Governance and Technology 2021, 92-94.
[413] Ibid, 97.

segmentation of data transfers to avoid triggering security assessment thresholds[414] and deficiencies in consent documentation or ethical review processes[415]. Failure to maintain backup and access obligations for Chinese partners can also lead to sanctions under the HGR framework.[416] Given these overlapping regimes, enforcement exposure arises across multiple regulatory domains, requiring strategies for integrated compliance and documentation. In the PDX scenario, the main risks are timely and complete NHC filings (incl providing backups), completeness and up-to-date TIAs/SCCs for any EU to China transfers and coherent documentation to demonstrate compliance and alignment across both jurisdictions.

The following concise overview by statute summarizes the link between compliance challenges, risks and consequences.

6.2.8.1. PIPL

Chapter IV PIPL allows the Cyberspace Administration of China (CAC) to order rectification of unlawful processing, confiscate illegal gains and impose administrative fines. In severe cases, regulators may suspend or terminate processing activities or revoke business licenses. The law also introduces personal liability for responsible individuals, including prohibitions on holding managerial positions. [417] Financial penalties can reach RMB 50 million[418] or 5% of the previous year's annual turnover for serious violations. Lesser infringements may result in fines up to RMB 1 million. These sanctions apply to breaches of general processing principles and to violations of cross-border transfer obligations under Article 38-40 PIPL. Failure to conduct a PIPIA or to file the required documentation for the Standard Contracts constitutes a material compliance risk in cross-border research settings. [419] Applied to the PDX collaboration, delayed or incomplete PIPIA preparation or late filing of Chinese Standard Contracts could trigger corrective orders or suspension of the relevant processing activities.

6.2.8.2. DSL and CSL

These laws add obligations on data classification, localization and incident response. [420]Regulatory authorities can impose corrective measures, confiscate illegal gains, suspend operations and revoke business licenses.[421] Authorities can further impose personal liability on responsible managers for serious breaches, including fines and administrative sanctions.[422] Unauthorized cross-border transfers without a security assessment can lead to fines up to RMB 1 million

[414] Article 3 SC Measures.
[415] Article 33 2023 Measures; Article 9 HGR Regulation.
[416] Article 14 and 33 MOST Implementing Rules.
[417] Article 63-67 PIPL.
[418] Which is roughly EUR 6,11 million as of 07. February 2026 (Exchange rate of RMB 1 = EUR 0,1222; 07.02.2026 by European Central Bank).
[419] Article 66 PIPL.
[420] Article 21 and 25 CSL; Article 21 DSL.
[421] Article 59 CSL.
[422] Article 66 CSL.

for CIIOs, combined with suspension or revocation of business licenses.[423] Violations of the DSL's data classification and security measures obligations[424] may trigger severe penalties up to RMB 10 million.[425] Failure to comply with incident response obligations can result in fines up to RMB 1 million and, in severe cases, suspension of operations.[426] The penalties scale with perceived impact on national security and public-interest. These escalation mechanisms create higher uncertainty for foreign research partners operating in China. For the PDX use case, a wrong classification of data or treating remote access not as an outbound transfer could be deemed unauthorized cross-border processing and expose the Chinese institute to penalties.

6.2.8.3. HGR Regulations and CBL

Violations of HGR approvals may lead to confiscation of samples/data, suspension or termination of research projects, and blacklisting of institutions, which restricts future filings and collaborations. Additional sanctions include administrative fines and, in severe cases, criminal liability under the Biosecurity Law. [427] The MOST Implementing Rules (Articles 14 and 33) mandate that Chinese partners have continuous, unrestricted access to research data and backups. Non-compliance can lead to additional sanctions, including administrative fines and restrictions on future research activities.[428] The CBL (Articles 36–38 and 53) introduces a security classification system for biotechnology activities and grants authorities the power to impose penalties for breaches that threaten national security or public health. Sanctions include fines up to RMB 10 million for severe violations, confiscation of materials and research outputs, and suspension of laboratory operations or revocations of permits.[429] In the PDX setting, failures to provide required backups or to restrict the Chinese partner's access to HGR-derived data may trigger the relevant enforcement mechanisms and affect subsequent NHC filings.

6.2.8.4. GDPR

The GDPR establishes a multi-level enforcement architecture including independent national supervisory authorities (SAs)[430], coordinated through the European Data Protection Board (EDPB)[431] and the cooperation and consistency mechanisms[432]. In intra-EU cross-border scenarios, the one-stop-shop mechanism designates a lead SA, while other SAs retain procedural

[423] Article 66 CSL.
[424] Article 21 DSL.
[425] Article 45-48 DSL.
[426] Article 53-55 CSL.
[427] Chapter IX CBL; Article 21–24 HGR Regulation.
[428] Chapter VI MOST Implementing Rules.
[429] Chapter IX CBL.
[430] Article 51-59 GDPR.
[431] See Article 68-76 GDPR.
[432] See Article 60-67 GDPR; *Lampert,* Data protection, privacy regulators and supervisory authorities, Bloomsbury Professional (2020), 32-33.

rights.[433] Under Article 58 GDPR, supervisory authorities may audit, access data, issue corrective orders and suspend data transfers, potentially halting EU-China data flows pending remediation.

Administrative fines (Article 83) must be "*effective, proportionate and dissuasive*"[434]. The GDPR distinguishes between two tiers: up to €10 million or 2% of global turnover for certain breaches, and up to € 20 million or 4% for core violations, including unlawful transfers under Chapter V.[435] Data subjects have layered remedies: complaints to SAs (Article 77 GDPR)[436], judicial review of SA decisions (Article 78 GDPR)[437], direct actions against controllers or processors (Article 79 GDPR)[438], and representation by qualified non-profits (Article 80 GDPR)[439].

Compensation for material and non-material damages (Article 82) requires proof of damage and causation. CJEU rulings confirm that distress may qualify.[440] These rulings are particularly relevant in biomedical research, where non-material harm (e.g. distress, loss of trust) might be alleged following security incidents.

The EDPB's Guidelines 04/2022 outline a five-step methodology for calculating fines, emphasizing context-specific factors such as risk profiles and safeguards like pseudonymization, which are critical in genetic research settings.[441] Finally, Member States may add penalties for infringements not covered by Article 83.[442] This creates a further compliance layer for institutions engaged in multi-jurisdictional research collaborations.[443]

For controllers in academic consortia, biobanks and the industry for which GDPR applies, typical enforcement exposures might include (i) insufficient legal basis or safeguards for special-category data[444], (ii) gaps in transparency towards data subjects[445], (iii) DPIA omissions for processing activities identified as posing of high-risk to the rights and freedoms of data subjects[446], (iv) inadequate security/TOMs including access restrictions and access management

---

[433] See Article 60 GDPR; EDPB, The EDPB: Guaranteeing the same rights for all, https://www.edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf (accessed 02.02.2026).
[434] Article 83(1) GDPR; *Lampert,* Data protection, privacy regulators and supervisory authorities, Bloomsbury Professional (2020), 34.
[435] *Lampert*, Data protection, privacy regulators and supervisory authorities, Bloomsbury Professional (2020), 35-37.
[436] Article 77 GDPR.
[437] Article 78 GDPR.
[438] Article 79 GDPR.
[439] Article 80 GDPR.
[440] Court of Justice of the European Union, Press Release No 191/23: Cybercrime: the fear of a possible misuse of personal data is capable, in itself, of constituting non-material damage, https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-12/cp230191en.pdf (accessed 29.12.2025).
[441] EDPB, Guidelines 04/2022, 2023.
[442] Article 84 GDPR.
[443] In intra-EU cross-border cases, the lead SA coordinates draft decisions under Article 60 GDPR. Concerned SAs may raise "relevant and reasoned objections" and the EDPB can adopt binding decisions under Article 65 GDPR to resolve disputes. A mechanism designed to avoid "forum shopping" and ensure EU-wide consistency. The CJEU's ruling C-645/19 clarified that non-SA may seize national courts only under GDPR exceptions, such as urgency (Article 66 GDPR) or local effects, in conformity with the GDPR's rules (Article 55-66 GDPR); See CJEU C-645/19, ECLI:EU:C:2021:483, Facebook Belgium, para. 11 and 75-77.
[444] See Article 6, 9 and 89 GDPR.
[445] Article 12-14 GDPR.
[446] Article 35 GDPR.

to genetic repositories[447], (v) data breach notification failures[448] and (vi) non-compliance with Chapter V obligations (e.g. incomplete TIAs, missing contractual or technical supplementary measures)[449], issues that might trigger upper-tier fines and transfer suspension under Article 58(2)(j) GDPR.

For the PDX collaboration, incomplete TIAs, inadequate TOMs for genetic-data processing and sharing or late or incomplete data breach reporting may result in transfer suspension under Article 58(2)(j) GDPR and other corrective orders.

6.2.8.5. Practical measures and strategies

To address enforcement and liability risks in EU-China collaborations the following strategies are recommended:

- Proactively monitor regulatory developments in both the EU and China, affecting compliance obligations or enforcement risks.
- Ensure early and complete submission of all required filings and approvals (e.g. NHC, CAC, ethics committees) to avoid administrative penalties, project suspension or even being blacklisted.
- Maintain robust documentation and evidence of compliance for all regulatory requirements, including specifically backup and access obligations for Chinese partners, consent documentation and ethical review processes.
- Engage with authorities for clarification and guidance if needed, for example via industry associations or law firms.
- Review and regularly update your compliance strategies to reflect new trends in enforcement, risk and best practices, including technical and organizational measures to reflect state-of-the-art technical developments.
- Train and educate responsible persons such as managers or researchers on personal liability risks and the importance of compliance with both EU and Chinese legislation.
- Avoid risk practices such as segmenting data transfers to circumvent security assessment thresholds.
- Additionally, monitor and consider also other countries' legislation, which might impact your organization or institute, such as the U.S. Biosecure Act.[450]

[447] Article 32 GDPR.
[448] Article 33-34 GDPR.
[449] Article 44-50 GDPR.
[450] The U.S. BIOSECURE Act of 2025 (H. R. 8333) bans all entities that are the recipient of federal funding in the US to use technology from a "biotechnology company of concern". Those companies seemingly impose a national security risk to the U.S. (see Sec. 2 (f) (2) (B) (iii) Biosecure Act). (Biosecure Act, U.S. Senate Bill S.3469, 119th Congress, https://www.congress.gov/bill/119th-congress/senate-bill/3469/text?s=2&r=3&q=%7B%22search%22%3A%22Biosecure%22%7D (accessed 01.02.2026)).

– In the PDX use case, these controls collectively reduce the likelihood that enforcement disrupts sequencing, analysis or material exchange and support continuity of the research collaboration.

7. Conclusion

This thesis has shown that cross-border preclinical oncology research collaborations between parties located in the EU and in China are shaped by fundamentally different regulatory philosophies.

The EU's framework is grounded in a rights-based conception of data protection that emphasizes fundamental rights and individual autonomy, whereas China's approach embeds personal data protection within a broader regulatory logic centered on national security and data sovereignty. These divergent principles manifest in strict collaboration requirements, data localization mandates and complex transfer rules on both sides. Taken together, these differences limit the extent to which procedural alignment is achievable unless targeted reforms are introduced.

The comparison demonstrates that these differences create substantial operational barriers for international research. The GDPR provides broad and dynamic consent models, research derogations and strong data subject rights, while China requires purpose-specific consent for each category of sensitive data and imposes stringent export controls for genetic material and biospecimens. The HGR Regulations and the Biosecurity Law further limit the transfers of human biospecimens, such as PDX models and genetic data, with recent guidance suggesting only limited flexibility. Accordingly, alignment at the project level generally relies on careful segmentation of roles, data categories and governance instruments, rather than on broader regulatory alignment.

Both jurisdictions apply layered cross-border transfer regimes – Chapter V GDPR with TIAs and SCCs, and China's four outbound transfer mechanisms with strict thresholds – which together result in multi-layered, often parallel compliance obligations. Data transfers from the EU to China frequently fail in practice due to Transfer Impact Assessment requirements, while transfers from China to the EU are constrained by HGR-based export controls. As a result, technical and organizational solutions that minimize the cross-border movement of raw data become essential, including local analytical environments and architectures that support privacy-enhancing approaches.

Beyond these legal and technical constraints, ethical and procedural hurdles further complicate collaborations. Consent models are difficult to harmonize and the absence of mutual recognition between ethics review systems leads to duplicated assessments, prolonged timelines and legal uncertainty. Collaboration requirements, including Joint Controller Agreements in the EU and mandatory Chinese partner involvement under the HGR regime, remain central

elements of compliance. These conditions create a compliance landscape that is highly demanding and may become operationally restrictive, particularly in projects that depend on efficient sequencing and analysis workflows.

The thesis proposes several strategies to mitigate these challenges. Early regulatory monitoring, precise role mapping, layered contractual frameworks and strong technical and organizational measures are essential. Awareness of exemptions – for example, the exclusion of immortalized cell lines or plasma from HGR oversight – can reduce administrative burdens. Where HGR Regulations apply, researchers must secure the required approvals, maintain continuous access for Chinese partners and implement robust safeguards such as multi-stage pseudonymization and encryption. These measures are derived directly from the comparative analysis of both systems and reflect legal necessity rather than operational preference.

While the findings are rooted in oncology, the underlying insights and compliance strategies are relevant across biomedical research involving sensitive genetic and health data. The analysis is subject to limitations, including the rapidly evolving legal environment, restricted access to some Chinese sources and the thesis' focus on EU-level rather than Member State-level law. Future research should explore stakeholder perspectives, evaluate new initiatives such as the proposal for the European Biotech Act[451], and examine mechanisms for harmonization and coordinated oversight.

Ultimately, enabling responsible and innovative international research requires not only robust legal frameworks but also practical mechanisms that facilitate cooperation, transparency and trust. Without progress toward pragmatic forms of regulatory alignment, global biomedical research is likely to remain constrained by fragmented rules and enduring legal uncertainty. In the meantime, carefully designed governance structures offer the most viable pathways to enabling compliant, ethically robust cross-border research.

[451] European Commission, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework of measures for strengthening Union's biotechnology and biomanufacturing sectors particularly in the area of health and amending Regulations (EC) No 178/2002, (EC) No 1394/2007, (EU) No 536/2014, (EU) 2019/6, (EU) 2024/795 and (EU) 2024/1938 (European Biotech Act), https://health.ec.europa.eu/document/download/ec1475b7-e3f9-409e-b927-fc7e69306a8c_en?filename=biotech_reg-com2025-1022_act_en.pdf (accessed 01.02.2026).

8. Abstract

8.1. English abstract

Preclinical cancer research is essential for the development of new therapies and for advancing our understanding of tumor biology. Its international orientation has become essential today. Genetic diversity and rare mutations can only be investigated through access to diverse patient populations. Many biomedical research projects rely on human biospecimens and personal data obtained from multiple countries. Funding programs such as Horizon Europe specifically support international collaborations, for example between the EU and China. At the same time, researchers face considerable challenges when collaborating and exchanging genetic data and biological samples. Different data protection laws (e.g. GDPR and PIPL), divergent ethical standards and consent models, regulatory barriers to the transfer of personal data and samples, as well as the operational complexity of implementing compliance requirements, complicate collaborations. This thesis provides a comparative analysis of the legal and ethical frameworks governing the cross-border exchange of genetic data, health data and biological samples between the EU and China. The central question is how the different legal regimes, particularly the GDPR, PIPL, DSL, CSL, CBL and HGR Regulations, affect research practice. Furthermore, the thesis addresses ethical aspects of informed consent and the protection of vulnerable groups, as well as practical challenges and pragmatic compliance strategies for research collaborations. The methodology is based on a legal analysis of the relevant provisions in both jurisdictions, complemented by a normative assessment of international and national ethical standards. A practical example (EU-China collaboration using PDX models) illustrates regulatory hurdles and presents concrete compliance strategies. The findings of this thesis show that the current legal landscape is characterized by high complexity and legal uncertainty. This may result in lengthy preparation times and increased resource requirements. The insights gained are relevant not only for oncological research, but also for international biomedical research as a whole and offer practical orientation for researchers, institutions and industry stakeholders in dealing with complex regulatory requirements.

8.2. German abstract

Präklinische Krebsforschung ist essenziell für die Entwicklung neuer Therapien und das Verständnis der Tumorbiologie. Ihre internationale Ausrichtung ist heute unverzichtbar. Genetische Diversität und seltene Mutationen können durch den Zugang zu unterschiedlichen Patientengruppen erforscht werden. Zahlreiche biomedizinische Forschungsprojekte sind auf Humanproben und personenbezogene Daten aus unterschiedlichen Ländern angewiesen. Förderprogramme wie Horizon Europe unterstützen gezielt internationale Kooperationen, z.B. zwischen der EU und China. Gleichzeitig stehen Forschende bei der Zusammenarbeit und dem Austausch genetischer Daten und biologischer Proben vor erheblichen Herausforderungen. Unterschiedliche Datenschutzgesetze (z.B. DSGVO und PIPL), divergierende ethische Standards und Einwilligungsmodelle, regulatorische Hürden beim Transfer von personenbezogenen Daten und Proben sowie die praktische Komplexität bei der Umsetzung von Compliance-Anforderungen erschweren die Zusammenarbeit. Diese Arbeit analysiert vergleichend die datenschutzrechtlichen und ethischen Rahmenbedingungen für den grenzüberschreitenden Austausch genetischer Daten, Gesundheitsdaten und biologischer Proben zwischen der EU und China. Im Mittelpunkt steht die Frage, wie die unterschiedlichen Rechtsrahmen, insbesondere DSGVO, PIPL, DSL, CSL, CBL und HGR-Regulierung, die Forschungspraxis beeinflussen. Des Weiteren widmet sich die Arbeit ethischen Aspekten der informierten Einwilligung und dem Schutz vulnerabler Gruppen sowie den praktischen Herausforderungen und pragmatischen Compliance-Strategien für den Forschungsalltag. Die Methodik basiert auf einer juristischen Analyse der einschlägigen Vorschriften beider Rechtsordnungen, ergänzt um eine normative Bewertung internationaler und nationaler ethischer Standards. Ein praxisnahes Beispiel (EU-China-Kollaboration mit PDX-Modellen) illustriert die regulatorischen Hürden und zeigt konkrete Compliance-Strategien auf. Die Ergebnisse der Arbeit verdeutlichen, dass die aktuelle Rechtslage von hoher Komplexität und rechtlicher Unsicherheit geprägt ist. Dies kann zu langen Vorlaufzeiten und erhöhtem Ressourcenbedarf führen. Die gewonnenen Erkenntnisse sind nicht nur für die onkologische Forschung, sondern auch für die internationale biomedizinische Forschung insgesamt relevant und bieten praxisnahe Orientierung für Wissenschaftler*innen, Institutionen und Akteure aus der Industrie im Umgang mit den komplexen regulatorischen Anforderungen.

9. References

9.1. Laws & regulations:

9.1.1. Chinese legal acts

2023 Measures for Ethical Review of Life Sciences and Medical Research Involving Human Beings (2023 Measures), issued 18.02.2023, original: https://www.nhc.gov.cn/qjjys/c100016/202302/6b6e447b3edc4338856c9a652a85f44b.shtml, English translation: https://www.lawinfochina.com/display.aspx?id=40963&lib=law (accessed 01.02.2026).

Beijing FTZ Data Outbound Negative List, issued 30.08.2024, original: https://www.beijing.gov.cn/zhengce/zhengcefagui/202409/t20240902_3787646.html, no English translation available, English summary: https://english.beijing.gov.cn/investinginbeijing/two_zones/updates/202409/t20240914_3891329.html (accessed 01.02.2026).

Chinese Biosecurity Law (CBL), issued 18.10.2020, amended 2024, original: http://www.xinhuanet.com/politics/2020-10/18/c_1126624481.htm, English translation: https://www.lawinfochina.com/display.aspx?id=43149&lib=law (accessed 01.02.2026).

Cybersecurity Law of the People's Republic of China (CSL), issued 07.11.2016, original: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm, English translation: https://www.lawinfochina.com/Display.aspx?LookType=1&Lib=law&Cgid=283838&Id=22826&SearchKeyword=&SearchCKeyword=&paycode= (accessed 01.02.2026).

Data Security Law of the People's Republic of China (DSL), issued 10.06.2021, original: https://www.moa.gov.cn/ztzl/zhnyzxd/zcfg/zybs/flfg/202501/P020250115579606737948.pdf, English translation: http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html (accessed 01.02.2026).

Decision of the Standing Committee of the National People's Congress on Amending the Cybersecurity Law of the People's Republic of China, issued 29.10.2025, original: https://www.gov.cn/yaowen/liebiao/202510/content_7046194.htm, English translation: https://www.lawinfochina.com/display.aspx?lib=law&id=45904 (accessed 01.02.2026).

Implementation Rules for the Regulations on the Management of Human Genetic Resources (MOST Implementing Rules), issued 01.06.2023, original: https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/fgzc/bmgz/202306/t20230601_186416.html, English translation: https://www.chinalawtranslate.com/en/Implementation-Rules-for-the-Regulations-on-the-Management-of-Human-Genetic-Resources/ (accessed 01.02.2026).

Measures for the Security Assessment of Data Exports, issued 07.07.2022, original: https://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm, English translation: https://www.chinalawtranslate.com/en/exdata-export-security/ (accessed 01.02.2026).

Measures on Standard Contracts for the Export of Personal Information (SC Measures), issued 03.02.2023, original: https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm, English translation: https://www.chinalawtranslate.com/en/personal-information-export-contract/ (accessed 01.02.2026).

Personal Information Protection Law (PIPL), issued 20.08.2021, original: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm, English translation: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (accessed 01.02.2026).

Provisions on Promoting and Regulating the Cross-Border Flow of Data, issued 22.03.2024, original: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm, English translation: https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/ (accessed 01.02.2026).

Regulation of the People's Republic of China on the Administration of Human Genetic Resources (HGR Regulation), issued 28.05.2019, original: https://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm, English translation: https://www.chinalawtranslate.com/en/p-r-c-regulation-on-the-management-of-human-genetic-resources/ (accessed 01.02.2026).

Regulations on Critical Information Infrastructure Security Protections, issued 30.07.2021, original: https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm, English translation: https://www.chinalawtranslate.com/en/Regulations-on-Critical-Information-Infrastructure-Security-Protections/ (accessed 01.02.2026).

Shanghai FTZ Data Export Negative List, issued 08.02.2025, original: https://www.lingang.gov.cn/upload/1/cms/content/editor/23c0db06-4b70-4c3d-a566-6ae4ddfb3bc5.pdf, no English translation available, English summary: https://www.lexology.com/library/detail.aspx?g=d9c7e592-9fb9-4bee-a3dd-3e2b8ac2f2a0 (accessed 01.02.2026).

9.1.2. EU legal acts

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012.

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199, 07.06.2021.

Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, 27.05.2014.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 07.06.2019.

Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013, OJ L 170, 12.05.2021.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 03.06.2022.

Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, OJ L 2025/327, 05.03.2025.

Treaty on the Functioning of the European Union, OJ C 115, 09.05.2008.

9.1.3. EU member state laws

Bundesdatenschutzgesetz (BDSG), BGBl I 2017, No 65.

Forschungsorganisationsgesetz BGBl 1981/341 version of BGBl I 52/2023.

9.1.4. US legal act

Biosecure Act, U.S. Senate Bill S.3469, 119th Congress, https://www.congress.gov/bill/119th-congress/senate-bill/3469/text?s=2&r=3&q=%7B%22search%22%3A%22Biosecure%22%7D (accessed 01.02.2026).

9.1.5. Legislative materials

Administrative Licensing for the Collection of Human Genetic Resources in China Service Guide, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/3b99b808608240878f866e53ce3a8e36/files/1746832742892_58540.pdf (accessed 01.02.2026), English translation available in Appendix 3.

Data Security Technology – Rules for Data Classification and Grading (GB/T 43697-2024), issued 21.03.2024, original: https://www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf?mc_cid=b0acb1c7ee&mc_eid=627c47469b (accessed 01.02.2026), English translation available in Appendix 3.

ENISA, EUCS – Cloud Services Scheme, issued December 2020, https://certification.enisa.europa.eu/document/download/c14f76c8-99e8-4900-a2c2-a412fa3ab071_en?filename=EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf (accessed 01.02.2026).

European Commission, Adequacy decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 01.02.2026).

European Commission, EU Cloud Certification Scheme, https://ec.europa.eu/newsroom/cipr/items/713799/en (accessed 01.02.2026).

European Commission, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework of measures for strengthening Union's biotechnology and biomanufacturing sectors particularly in the area of health and amending Regulations (EC) No 178/2002, (EC) No 1394/2007, (EU) No 536/2014, (EU) 2019/6, (EU) 2024/795 and (EU) 2024/1938 (European Biotech Act), https://health.ec.europa.eu/document/download/ec1475b7-e3f9-409e-b927-fc7e69306a8c_en?filename=biotech_reg-com2025-1022_act_en.pdf (accessed 01.02.2026).

FAQ regarding Human Genetic Resource Management, issued 27.03.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/39a747744f2242068fdaf39b0452e11e.shtml (accessed 01.02.2026), English translation in Appendix 3.

Information Security Technology – Guide for Health Data Security (GB/T 39725-2020), issued 14.12.2020, original: http://www.phic.org.cn/zcbz/bzypj/bzgf/gjbz/202408/P020240819570037182147.pdf, English translation: https://www.codeofchina.com/standard/GBT39725-2020.html (accessed 01.02.2026).

Q&A on Data Export Security Management Policies, issued 09.04.2025, original: https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm (accessed 01.02.2026), English translation available in Appendix 3.

Q&A on Data Outbound Security Management Policy, issued 31.10.2025, original: https://www.cac.gov.cn/2025-10/31/c_1763633376984070.htm (accessed 01.02.2026), English translation available in Appendix 3.

Q&A on Issues Related to the Management of Human Genetic Resources (Part I), issued 01.04.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202504/e9974e2f7a324590947485b74d796b71.shtml (accessed 01.02.2026), English translation available in Appendix 3.

Q&A on Issues Related to the Management of Human Genetic Resources (Part II), issued 09.04.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202504/17f9863c65c742d4b31ccb745e26082a.shtml (accessed 01.02.2026), English translation available in Appendix 3.

Q&A on Issues Related to the Management of Human Genetic Resources (Part V), issued 11.10.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202510/f04ebf5bc27a47e5a1ac6f370b3c5ec3.shtml (accessed 01.02.2026), English translation available in Appendix 3.

Standard Contract for Cross-border Transfer of Personal Information, https://www.glo.com.cn/UpLoadFile/Files/2023/3/1/11535343a7a943e1-f.pdf (accessed 01.02.2026).

9.2. Court rulings

CJEU C-413/23 P, ECLI:EU:C:2025:723, EDPS v. SRB.

CJEU C-645/19, ECLI:EU:C:2021:483, Facebook Belgium.

CJEU C-604/22, ECLI:EU:C:2024:214, IAB Europe.

CJEU C-311/18, ECLI:EU:C:2020:559, Schrems II.

ECHR 07.12.1976, 5493/72, Handyside v. the UK.

ECHR 26.03.1987, 9248/81, Leander v. Sweden.

9.3. Guidelines, codes and standards

Agencia Española de Protección de Datos, Código de Conducta regulador del tratamiento de datos personales, published February 2022, https://www.aepd.es/documento/codigo-conducta-farmaindustria-cc-0007-2019.pdf (accessed 01.02.2026).

CNIL, Practical Guide, Transfer Impact Assessment, issued January 2025, https://www.cnil.fr/sites/cnil/files/2025-01/guide_tia.pdf (accessed 01.02.2026).

CNIL, Transfer Impact Assessment (TIA): the CNIL publishes the final version of its guide, published on 09.07.2025, https://www.cnil.fr/en/transfer-impact-assessment-tia-cnil-publishes-final-version-its-guide (accessed 01.02.2026).

CIOMS, International Ethical Guidelines for Health-related Research Involving Humans, Geneva 2016, https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf (accessed 01.02.2026).

EDPB, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, adopted on 23.07.2020.

EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25.05.2018.

EDPB, Guidelines 03/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, adopted on 12.11.2019.

EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 04.05.2020.

EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 20.07.2021.

EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1, adopted on 24.05.2023.

EDPB, Guidelines 01/2025 on Pseudonymisation, adopted on 16.01.2025.

EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18.06.2021.

EDPB, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, Final Report, published 07.09.2021.

EDPB, Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, published 17.07.2020, https://www.edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en (accessed 01.02.2026).

EDPS, A Preliminary Opinion on data protection and scientific research, published 06.01.2020, https://www.edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf (accessed 01.02.2026).

European Commission, New Standard Contractual Clauses – Questions and Answers overview, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (accessed 01.02.2026).

European CRO Federation, GDPR Code of Conduct, https://eucrof.eu/gdpr-code-of-conduct/ (accessed 01.02.2026).

European Medicines Agency, ICH E6 Good Clinical Practice – Scientific Guideline, issued 1996, last amended 2025, https://www.ema.europa.eu/en/ich-e6-good-clinical-practice-scientific-guideline (accessed 01.02.2026).

Ferlay/Ervik/Lam/Laversanne/Colombet/Mery/Piñeros/Znaor/Soerjomataram/Bray, Global Cancer Observatory: Cancer Today, World, https://gco.iarc.who.int/media/globocan/factsheets/populations/900-world-fact-sheet.pdf (accessed 01.02.2026).

Ferlay/Ervik/Lam/Laversanne/Colombet/Mery/Piñeros/Znaor/Soerjomataram/Bray, Global Cancer Observatory: Cancer Today, China, https://gco.iarc.who.int/media/globocan/factsheets/populations/160-china-fact-sheet.pdf (accessed 01.02.2026).

Faymann/Anwana/Barud/Wagner/Polychronopoulos, Digital health innovations — Good practice guide for obtaining consent for the use of personal health information for research and innovations, https://www.cencenelec.eu/media/CEN-

CENELEC/News/Workshops/2023/2023-03-15%20-%20Digital%20Health/draftcwa.pdf (accessed 01.02.2026).

Garante per la protezione dei dati personali, Regione Veneto - Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica, published 14.01.2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9535402 (accessed 01.02.2026).

Innovative Health Initiative, Code of Practice on Secondary Use of Medical Data in Scientific Research Projects, published 27.04.2014, https://www.ihi.europa.eu/sites/default/files/uploads/documents/reference-documents/CodeofPractice_SecondaryUseDRAFT.pdf (accessed 01.02.2026).

International Organization for Standardization, ISO Standards for Biobanking, ISO 20387:2018, issued 2018, https://www.iso.org/standard/67888.html (accessed 01.02.2026).

National Institutes of Health, Guiding Principles for Ethical Research, https://www.nih.gov/health-information/nih-clinical-research-trials-you/guiding-principles-ethical-research (accessed 01.02.2026).

OECD, Recommendation of the Council on Human Biobanks and Genetic Research Databases, adopted 22.10.2009, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0375 (accessed 01.02.2026).

Okręgowa Izba Lekarska w Szczecinie, KODEKS POSTĘPOWANIA DLA SEKTORA OCHRONY ZDROWIA, issued 23.11.2020, https://www.oil.szczecin.pl/upload/files/KODEKS%20POSTEPOWANIA%20DLA%20SEKTORA%20OCHRONY%20ZDROWIA.pdf (accessed 01.02.2026).

TeleTrust/ENISA, Guideline “State of the art” in IT security, Technical and organizational measures, adopted in 2025, https://www.teletrust.de/fileadmin/user_upload/2025-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf (accessed 01.02.2026).

The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, The Belmont Report, Ethical Principles and Guidelines for the Protection of Human Subjects of Research, issued 18.04.1979, https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf (accessed 01.02.2026).

UNESCO, Universal Declaration on Bioethics and Human Rights, adopted 19.10.2005, https://www.unesco.org/en/legal-affairs/universal-declaration-bioethics-and-human-rights?hub=387 (accessed 01.02.2026).

World Medical Association, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants, issued in June 1964, last amended October 2024, https://www.wma.net/policies-post/wma-declaration-of-helsinki/ (accessed 01.02.2026).

World Medical Association, Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, issued in October 2002, last amended October 2016, https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/ (accessed 01.02.2026).

World Health Organization, Ethics and governance of artificial intelligence for health, adopted 28.06.2021, https://www.who.int/publications/i/item/9789240029200 (accessed 01.02.2026).

9.4. Books and articles

Alser/Almadhoun/Nouri/Alkan/Ayday, Can you Really Anonymize the Donors of Genomic Data in Today's Digital World? in: *Garcia-Alfaro/Livraga/Roudier/Soriente* (eds.), Data Privacy Management, and Security Assurance *(*DPM 2015, QASA 2015), Lecture Notes in Computer Science (2016), 237-244.

Annaratone/De Palma/Bonizzi/Sapino/Botti/Berrino/Mannelli/Arcella/Di Martino/Steffan/Daidone/Canzonieri/Parodi/Paradiso/Barberis/Marchiò, Basic principles of biobanking: from biological samples to precision medicine for patients, Virchows Archiv 2021, 233-246.

Beauchamp/Childress, Principles of Biomedical Ethics, 8th ed (2019).

Bersanelli/Mosca/Remondini/Giampieri/Sala/Castellani/Milanesi, Methods for the integration of multi-omics data: mathematical aspects, BMC Bioinformatics 2016, 167-177.

Bibbins-Domingo/Brubaker/Curfman, Editor's Note: The 2024 Revision to the Declaration of Helsinki: Modern Ethics for Medical Research, Journal of the American Medical Association 2025, 30-31.

Borg/Caruana, Alternative Legal Bases for Processing Health Data for Scientific Research Purposes, Masaryk University Journal of Law and Technology 2024, 3-26.

Bray/Laversanne/Sung/Ferlay/Siegel/Soerjomataram/Jemal, Global cancer statistics 2022: GLOBOCAN estimates of incidence and mortality worldwide for 36 cancers in 185 countries, CA: A Cancer Journal for Clinicians 2024, 229-263.

Bray/Laversanne/Weiderpass/Soerjomataram, The ever-increasing importance of cancer as a leading cause of premature death worldwide, Cancer 2021, 3029-3030.

Cai/Bigdeli/Kretzschmar/Li/et al., Retraction Note: 11,670 whole-genome sequences representative of the Han Chinese population from the CONVERGE project, Scientific Data 2020, 1.

Cavaleri/Sousa/Hacker/Higgs/Lumpkin/Maia/et al., A roadmap for fostering timely regulatory and ethics approvals of international clinical trials in support of global health research systems, Lancet Global Health 2025; e769-e777.

Chen, Research on Data Sovereignty Rules in Cross-border Data Flow and Chinese Solution, US-China Law Review 2021, 261-273.

Chen/Berkman/Hull, Recontacting participants for expanded uses of existing samples and data: a case study, Genetics in Medicine 2017, 883-889.

Chen/Li, Is cross-border transfer of China's human genetic data an impossible mission? Human Genetics 2025, 1-11.

Chen/Sun, Understanding the Chinese Data Security Law, International Cybersecurity Law Review 2021, 209-221.

Creemers, China's emerging data protection framework, Journal of Cybersecurity 2022, 1-12.

Das/Das, Orthotopic PDX and CDX Mice Model for Cancer Stem Cell Research, in: *Pathak/Banerjee/Bisgin* (eds.), Handbook of Animal Models and its Uses in Cancer Research (2023) 503-526.

Dove/Garattini, Expert perspectives on ethics review of international data-intensive research: Working towards mutual recognition, Research Ethics 2018, 1-25.

Dove/Townend/Meslin/Bobrow/Littler/et al., Research Ethics. Ethics review for international data-intensive research, Science 2016, 1399-1400.

Duguet/Herveg, Safeguards and Derogations Relating to Processing for Scientific Purposes: Article 98 Analysis for Biobank Research, in: *Slokenberga/Tzortzatou/Reichel (eds.),* GDPR and Biobanking, Law, Governance and Technology (2021) 105-120.

Durmus, Praktische Durchführung von Transfer Impact Assessments (TIA), Datenschutz-Berater 2023, 48.

Gabauer/Höller, Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down?, Datenschutz Konkret 2020, 80-82.

Gang/Peng, China Releases Document on Ethics Review of Life Sciences: Comments and Compliance Guideline, Biotechnology Law Report 2023, 149-153.

Gao, A Battle of the Big Three?-Competing Conceptualizations of Personal Data Shaping Transnational Data Flows, Chinese Journal of International Law 2023, 707-787.

Golland, Anforderungen an Transfer Impact Assessments bei Datentransfers in unsichere Drittländer, Datenschutz-Berater 2021, 229-231.

Greely, CRISPR'd babies: human germline genome editing in the 'He Jiankui affair', Journal of Law and the Biosciences 2019, 111-183.

Guo/Li, Cross-border data flow in China: Shifting from restriction to relaxation? Computer Law & Security Review 2025, 1-12.

Haimberger, Datenschutz in der medizinischen und pharmazeutischen Forschung, Dissertation, Universität Wien (2023).

Hallinan, Broad consent under the GDPR: an optimistic perspective on a bright future, Life Sciences, Society and Policy 2020, 1-18.

Hänold, Die Zuverlässigkeit eines "broad consent" in der medizinischen Forschung – a never ending story? ZD-Aktuell 2020, beck-online.beck.de (accessed 01.02.2026).

He, When data protection norms meet digital health technology: China's regulatory approaches to health data protection, Computer Law & Security Review 2022, 1-14.

Herbst, Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, Datenschutz und Datensicherheit 2016, 371-375.

Jung, Human Tumor Xenograft Models for Preclinical Assessment of Anticancer Drug Development, Toxicological Research 2014, 1-5.

Kaye/Whitley/Lund/Morrison/Teare/Melham, Dynamic consent: a patient interface for twenty-first century research networks, European journal of human genetics 2015, 141-146.

Kennedy, The "Gold" Standard – China finalises the long-anticipated Standard Contract under the Personal Information Protection Law, Computer Law & Security Review 2023, 2.

Khandelwal/Girotti/Smowton/Taylor/et al., Next-Generation Sequencing Analysis and Algorithms for PDX and CDX Models, Molecular Cancer Research 2017, 1012-1016.

Knyrim/Gerhalter, Art 46 DSGVO. Datenübermittlung vorbehaltlich geeigneter Garantien, in: Knyrim (ed.), Der DatKomm (2023).

Krt, Cell Line Establishment Methods: Biomedical Research Advances and Challenges, Stem Cell Research and Regenerative Medicine 2023, 103–105.

Kurihara/Kerpel-Fronius/Becker/Chan/Nagaty/Naseem/Schenk/Matsuyama/Baroutsou, Declaration of Helsinki: ethical norm in pursuit of common global goals, frontiers in Medicine 2024, 1-5.

Lampert, Data protection, privacy regulators and supervisory authorities, Bloomsbury Professional (2020).

Li/Cong/Liu, Research under China's personal information law, Science 2022, 713-715.

Marnau/Berrang/Humbert, Anonymisierungsverfahren für genetische Daten, Datenschutz und Datensicherheit 2018, 83-88.

Matar/Hansson/Slokenberga/Panagiotopoulos/Chassang/Tzortzatou/Pormeister/Uhlin/Cardone/Beauvais, A proposal for an international Code of Conduct for data sharing in genomics, Developing World Bioethics 2022, 344-357.

Mathews/Rabin/Quain/Campbell/Collyar/Hlubocky/Isakoff/Peppercorn, Secondary Use of Patient Tissue in Cancer Biobanks, The Oncologist 2019, 1577-1583.

McKibbin/Shabani, Genomic Data as a National Strategic Resource: Implications for the Genomic Commons and International Data Sharing for Biomedical Research and Innovation, The Journal of Law, Medicine & Ethics 2023, 301-312.

Melosky/Kambartel/Häntschel/Bennetts/Nickens/Brinkmann/Kayser/Moran/Cappuzzo, Worldwide Prevalence of Epidermal Growth Factor Receptor Mutations in Non Small Cell Lung Cancer: A Meta-Analysis, Molecular Diagnosis & Therapy 2022, 7-18.

Midha/Dearden/McCormack, EGFR mutation incidence in non-small-cell lung cancer of adenocarcinoma histology: a systematic review and global map by ethnicity (mutMapII), Am J Cancer Res 2015, 2892-2911.

Mirabelli/Coppola/Salvatore, Cancer Cell Lines Are Useful Model Systems for Medical Research, Cancers 2019, 1-18.

Moctezuma-Ramirez/Dworaczyk/Whitehorn/Li/Cardoso/Elgalad, Designing an In Vivo Preclinical Research Study, Surgeries 2023, 544-555.

Mok, Secretariat of the National Information Security Standardization Technical Committee, Cybersecurity Standard Practice Guidelines: Specifications for the Security Certification of Cross-Border Personal Information Processing Activities V2.0 (Draft for Comments), China Law & Practice 2022, https://www.proquest.com/docview/2737578271?parentSessionId=eLb%2BAjUO%2FbVCdzAc5ykU15ronhaMRn1PZ%2Bs4a%2F1Bol0%3D&pq-origsite=primo&accountid=14682&sourcetype=Trade%20Journals (accessed 01.02.2026).

Morton/Houghton, Establishment of human tumor xenografts in immunodeficient mice, Nature Protocols 2007, 247-250.

Nagai/Nakazawa/Akabayashi, The creation of the Belmont Report and its effect on ethical principles: a historical study, Monash Bioethics Reviews 2022, 157-170.

Parasol, AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws, Cambridge University Press (2021).

Prictor/Teare/Kaye, Equitable Participation in Biobanks: The Risks and Benefits of a "Dynamic Consent" Approach, frontiers in Public Health 2018, 1-6.

Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, Law, Innovation and Technology 2018, 1-35.

Reuter/Voigt, Die neuen EU-Standardvertragsklauseln - Best Practice, Datenschutzberater 2022, 309.

Rothstein/Zawati/Thorogood/Beauvais/Joly/Brothers/et al., Streamlining ethics review for international health research, Science 2022, 825-826.

Shabani/Borry, Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation, European Journal of Human Genetics 2018, 149-156.

Shabani/Marelli, Re-identifiability of genomic data and the GDPR, EMBO reports 2019, 1-5.

Si/Tao/Wu/Ma/Li/Feng/Song/Kong/Zhou, Tumor organoids in immunotherapy: from disease modeling to translational research, The Journal for ImmunoTherapy of Cancer 2025, 1-14.

Siolas/Hannon, Patient Derived Tumor Xenografts: transforming clinical samples into mouse models, Cancer Research 2013, 5315-5319.

Sirugo/Williams/Tishkoff, The Missing Diversity in Human Genetic Studies, Cell 2019, 26-31.

Staunton, Individual Rights in Biobank Research Under the GDPR, in: *Slokenberga/Tzortzatou/Reichel* (eds.), GDPR and Biobanking, Law, Governance and Technology (2021).

Staunton/Slokenberga/Parziale/Mascalzoni, Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research, frontiers in Genetics 2022, 1-10.

Wang/Du, Cross-Border Health Data Transfer for Scientific Research Purposes in China: Legislation, Practice, and Challenges, in: *Compagnucci/Fenwick* (eds.), International Transfers of Health Data: A Global Perspective, Perspectives in Law, Business and Innovation, Springer 2025, 186-210.

Wang/Gregg/Du, Regulatory barriers to US–China collaboration for population health research, Cell Genomics 2022, 1-5.

Wang/Jiang/Miao/Fang/et al., Targeting rare tumors: new focus for clinical research in China, EMBO olecular medicine 2023, 1-4.

Wang/Wang/Zhang, Bioethics in China's Biosecurity Law: forms, effects, and unsettled issues, Journal of Law and the Biosciences 2021, 1-15.

Wildiers/Adam/O'Reilly/et al., Enhancing Clinical Cancer Research Through Sharing of Data and Biospecimens, JAMA Oncology 2025, https://jamanetwork.com/journals/jamaoncology/article-abstract/2843053 (accessed 19.12.2025).

Yang/Wang/Wang/Zhang/Wang, Tumor organoids for cancer research and personalized medicine, Cancer Biology & Medicine March 2022, 319-332.

Yun, China's Data Sovereignty and Security: Implications for Global Digital Borders and Governance, Chinese Political Science Review 2025, 178-203.

9.5. Online sources

BBMRI-ERIC, A Code of Conduct for Health Research, https://code-of-conduct-for-health-research.eu/ (accessed 20.12.2025).

BDI, European Cybersecurity Certification Scheme for Cloud Services (EUCS), https://english.bdi.eu/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs (accessed 23.12.2025).

Carnegie Mellon University, What is Computational Biology, https://cbd.cmu.edu/about-us/what-is-computational-biology.html (accessed 17.08.2025).

Court of Justice of the European Union, Press Release No 191/23: Cybercrime: the fear of a possible misuse of personal data is capable, in itself, of constituting non-material damage, https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-12/cp230191en.pdf (accessed 29.12.2025).

Court of Justice of the European Union, Press Release No 91/20, issued 16.07.2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (accessed 08.12.2025).

Covington, China's NHC Issues Updated Guidelines on Human Genetic Resources Management, https://www.covingtonblogs.com/2025/04/18/chinas-nhc-issues-updated-guidelines-on-human-genetic-resources-management (accessed 01.02.2026).

DataGuidance, USA: AGs sue to prevent 23andMe from selling customer genetic data without consent, https://www.dataguidance.com/news/usa-ags-sue-prevent-23andme-selling-customer-genetic (accessed 01.02.2026).

DLA Piper, CHINA: Amendments to Cybersecurity Law Effective 1 January 2026, https://privacymatters.dlapiper.com/2025/11/china-amendments-to-cybersecurity-law-effective-1-january-2026 (accessed 03.01.2026).

DLA Piper, Collection and Processing in Russia, https://www.dlapiperdataprotection.com/?t=collection-and-processing&c=RU#insight (accessed 01.02.2026).

DLA Piper, Data Protection Laws in China, https://www.dlapiperdataprotection.com/index.html?c=CN (accessed 01.02.2026).

EBF, Joint Statement on EUCS, https://www.ebf.eu/wp-content/uploads/2023/11/Joint-Statement-on-EUCS.pdf (accessed 23.12.2025).

EDPB, The EDPB: Guaranteeing the same rights for all, https://www.edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf (accessed 02.02.2026).

Eckhardt/Hoffmann, EU Cloud Certification at an Impasse, https://www.cep.eu/eu-topics/details/eu-cloud-certification-at-an-impasse.html (accessed 19.10.2025).

European Commission, EU and China launch Cross-Border Data Flow Communication Mechanism, https://policy.trade.ec.europa.eu/news/eu-and-china-launch-cross-border-data-flow-communication-mechanism-2024-08-28_en (accessed 20.12.2025).

European Commission, Press Release: New measures to make EU health sector more innovative, competitive and resilient, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_3077 (accessed 19.12.2025).

European Commission (CORDIS), Toward enhancing activities of European institutions in the FDUSCC-IM cancer research joint institute in China, https://cordis.europa.eu/article/id/92712-euchina-collaboration-combats-cancer (accessed 31.10.2025).

European DIGITAL SME Alliance, Changes to the EU Cloud Services Cybersecurity Certification Scheme put EU citizens' data at risk: A Call for Digital Sovereignty, https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty (accessed 19.10.2025).

European DIGITAL SME Alliance, Policy Paper, EU Certification Scheme for Cloud Services: An opportunity for Europe's Digital Sovereignty, https://www.digitalsme.eu/digital/uploads/Policy-Paper-EU-Certification-Scheme-for-Cloud-Services.pdf (accessed 23.12.2025).

European Research Council, Ethics guidance, https://erc.europa.eu/manage-your-project/ethics-guidance (accessed 09.11.2025).

Gamvros/Wang, Data Protection Report, “Am I a CII operator?” – New regulation in China provides more clarity, https://www.dataprotectionreport.com/2021/08/am-i-a-cii-operator-new-regulation-in-china-provides-more-clarity/ (accessed 20.12.2025).

Global Network Initiative, Data localization: A Global Threat to Human Rights Online, https://globalnetworkinitiative.org/data-localization-a-global-threat-to-human-rights-online/ (accessed 23.12.2025).

Huld, China Clarifies Cross-Border Data Transfer Rules: Key Takeaways from Official Q&A (I), China Briefing, https://www.china-briefing.com/news/china-clarifies-cross-border-data-transfer-rules-official-qa/ (accessed 05.10.2025).

Huld, How to Conduct a Personal Information Protection Impact Assessment in China, https://www.china-briefing.com/news/how-to-conduct-a-personal-data-impact-assessment-in-china/ (accessed 03.01.2026).

IAPP-EY, Annual Privacy Governance Report 2019, https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt4eeb51e4cacccc06/Governance_Report_2019.pdf (accessed 07.02.2026).

International Services Shanghai, New list to aid outbound data flows, https://english.shanghai.gov.cn/en-Latest-WhatsNew/20240520/e66e1b5b4f894f6b9c6c1f1dcecc0a76.html (accessed 20.09.2025).

Mayer Brown, China Finalises Amendments to the Cybersecurity Law What Businesses Need to Know Before 1 January 2026, https://www.mayerbrown.com/en/insights/publications/2025/12/china-finalises-amendments-to-the-cybersecurity-law-what-businesses-need-to-know-before-1-january-2026 (accessed 03.01.2026).

Medizinische Universität Wien, EGFR-Mutationen reagieren unterschiedlich auf Behandlung, https://www.meduniwien.ac.at/web/ueber-uns/news/detail/egfr-mutationen-reagieren-unterschiedlich-auf-behandlung/ (accessed 19.12.2025).

National Cancer Institute, Biospecimen Best Practice Introduction, https://dctd.cancer.gov/data-tools-biospecimens/biospecimens-biobanks/resources/best-practices/biospecimen-resources/intro (accessed 31.10.2025).

Urząd Ochrony Danych Osobowych, The first Polish code of conduct compliant with the GDPR approved, https://uodo.gov.pl/en/553/1325 (accessed 01.02.2026).

WMA, Revised Declaration of Helsinki adopted by the global medical community, strengthening ethical standards in clinical research involving humans, https://www.wma.net/news-post/revised-declaration-of-helsinki-adopted-by-the-global-medical-community-strengthening-ethical-standards-in-clinical-research-involving-humans/ (accessed 04.01.2026).

10. Appendices

10.1. Appendix 1: Comparative table: GDPR vs. China's data protection framework

Aspect	EU (GDPR)	China (PIPL, DSL, CSL, HGR, CBL)
Territorial scope	Applies to processing in the context of an EU establishment and targeting/monitoring of persons in the EU (Article 3(1) and (2) GDPR)	PIPL applies inside China and extraterritorially when processing outside China provides products/services to persons in China or analyzes their behavior (Article 3 PIPL); DSL extends extraterritorially where activities endanger national security/public interest
Material scope	GDPR applies to personal data; anonymous data excluded (Article 2(1) and 4(1) GDPR, Recital 26 GDPR)	PIPL covers personal information; anonymous information excluded (Article 4 PIPL)
Definition of genetic data	Genetic data is a special category (Article 4(13) and Article 9 GDPR; Recital 34)	Article 2 HGR Regulations (covers human biospecimen and derived data) Sensitive personal information includes health and medical data (Article 28 and 29 PIPL)
Roles	Controller/Processor/Joint Controller	Personal Information Processor (Article 4 PIPL) analogous to GDPR's controller
Legal Basis (genetic data/health data)	Special categories require Article 9(2) GDPR legal bases (e.g. consent (a), public interest (g), research (j); derogation for scientific research in Article 89 GDPR including safeguards)	Article 13 PIPL (consent, contract, legal duties, emergencies, public interest); no research exemption; sensitive data requires separate consent (Article 28-29 PIPL)
Consent models	Explicit consent (Article 9 (2) (a) GDPR); Broad consent allowed (Recital 33); Dynamic consent recommended by EDPB	Purpose-specific separate consent for sensitive data (Article 28 and 29 PIPL). For HGR activities, informed consent required (Article 9 HGR Regulation); oral consent allowed if documented (Article 9 HGR Reg.; Article 33 2023 Measures)
Transparency obligations	Article 12-14 GDPR (clear, accessible, information on processing, recipients, rights, etc.)	Article 30 PIPL (including purpose, necessity, impact on rights); Article 36 2023 Measures (detailed disclosures for biospecimens: type, quantity, use, storage, reuse, destruction)
Research exceptions and safeguards	Article 89 GDPR (pseudonymization, TOMs, ethic review); Member state laws (e.g. Austrian FOG)	No explicit research exemptions; strict compliance with consent and ethical review (Article 8 MOST Implementing Rules)
Data subject rights	Access, rectification, erasure, restriction, objection, data portability (Article 15-22 GDPR); derogations possible for research (Article 89 GDPR)	Similar rights under PIPL (Article 44-49 PIPL) but limited in practice; strong state oversight
Pseudonymization and anonymization	Pseudonymization (Article 4(5) GDPR), anonymous data out of scope (Recital 26). Genetic data anonymization debated; safeguards encouraged (EDPB Guidelines)	Pseudonymization not explicitly define; anonymized data excluded from PIPL scope (Article 4 PIPL); TOMs like encryption/de-identification referenced in Chinese Standard Contract obligations
Cross-border data transfers	Chapter V GDPR: Adequacy (Article 45 GDPR); EU-SCCs (Article 46(2)(c) GDPR); BCRs	Article 38-40 PIPL: CAC Security Assessment, Chinese SC (SC Measures), Certifica-

	(Article 47 GDPR); Codes of Conduct/Certification (Article 40–42 GDPR); Derogations (Article 49 GDPR)	tion; PIPIA mandatory; thresholds: ≥1 million individuals or ≥ 10.000 sensitive data (Article 7 Provisions 2024)
Transfer assessments	TIA mandated post-Schrems II for Article 46 GDPR transfer safeguards	PIPIA required for Chinese SC, certification and security assessment; filing within 10 working days; re-filing when material changes occur (e.g. Article 7-9 SC Measures; Standard Contract Articles)
Data localization	No general localization requirement	Article 37 CSL: CIIOs must store personal and Important Data in China; Article 40 PIPL: Large volumes of PI or sensitive PI (≥ 1 million or ≥ 100.000) must be stored in China; HGR export restrictions (Article 7, 21 and 24 HGR Regulations)
Sector-specific scope/definitions (HGR)	n.a.	Article 2 and 3 HGR Regulation: HGR = human genetic materials and human genetic information (derived data). Applies to collection, use, preservation, provision
Foreign collaboration & export controls (HGR)	Collaborations (domestic and foreign) between two or more controllers require concluding a JCA (Article 26 GDPR)	HGR Reg. Article 7, 21-24: foreign entities must partner with Chinese institutions; joint application to MOST for international collaborations; approvals/filings; continuous access/backup for Chinese party (Article 14 and 33 MOST Implementing Rules). Export/transport of HGR requires prior approval
Ethical oversight	Independent IRBs; research safeguards under Article 89 GDPR; ethics review encouraged/required by Member State laws and biobank practice	Mandatory ethics review for HGR and human-involving life science/medical research: Measures 2023; Article 8 MOST Implementing Rules; dual approval for international projects (Article 31 MOST Implementing Rules). Confidentiality duties for committees (Article 10 SC Measures)
Philosophical Approach	Fundamental rights-based; individual autonomy	Data sovereignty and national security; genetic data as a strategic resource (Article 53 CBL rationale)
Supervisory / enforcement architecture	National Supervisory Authorities (Article 51–54 GDPR), with investigative/corrective powers (Article 58 GDPR); EDPB for consistency (Article 63 GDPR); judicial remedies & compensation (Article 77–82 GDPR)	CAC (cross-border/data/CSL matters); NHC (HGR approvals/oversight); ethics committees under Measures 2023; local/sector regulators
Investigative & corrective powers	Article 58 GDPR: orders to comply, access, audits, ban processing/transfers, rectification/erasure, administrative fines.	PIPL regulators can order rectification, confiscate unlawful gains, suspend/terminate services, sanction responsible individuals (as summarized: PIPL Ch. VII). HGR/CBL allow confiscation of materials/data, suspension/termination, blacklisting
Fines & penalties	Article 83 GDPR: up to € 20 million or 4% global annual turnover (higher of), or € 10 million/2% for lower tier; Article 84 GDPR (Member State penalties)	PIPL Ch. VII (enforcement/penalties: significant fines, confiscation, suspensions, personal liability/role bans); DSL/CSL: fines, suspension, license revocation, confiscation for classification/localization/incident breaches (as summarized); HGR/CBL: fines, confiscations, approval cancellations, pro-

		ject suspension for unlawful collection/preservation/export or non-compliance with joint submission/ethics

10.2. Appendix 2: Transfer Impact Assessment for PDX use case addressed in Chapter 6

The EDPB has issued a six-step[452] methodology for conducting a TIA:

Step 1: Know your transfers[453]

In the use case, genetic data as well as clinical health data are transferred from an EU-based pharmaceutical company to a Chinese oncology institute for validation and joint research. The Chinese institute acts as a controller for the biospecimen collection, PDX generation and sequencing. The EU company is the controller for compound testing and the import of personal data and HGR information from Chinese individuals. Both parties jointly conduct research.

Step 2: Identify the transfer tool used[454]

China lacks an adequacy decision.[455] Furthermore we assume that no approved code of conduct pursuant to Article 40 GDPR has been adopted covering the given transfer and the research parties do not qualify as groups of undertakings, making Binding Corporate Rules (BCRs) unavailable.[456] The preferred transfer mechanisms would be Standard Contractual Clauses (SCC), either Module 1 (C2C) in case the Chinese institute is considered a data controller or Module 2 (C2P) if it is a processor.[457]

Step 3: Assess whether the transfer mechanism is effective[458]

The SCC must effectively preserve the level of data protection guaranteed under GDPR, ensuring that it is not compromised in practice during the transfer to Mainland China or when processed there.[459] Chinese law (PIPL, DSL, HGR Regulations) impose strict data localization and export controls, especially for HGR data. Public authorities may access data for national security reasons, potentially undermining SCC safeguards. The TIA must consider those risks, as well as the volume and type of data and any sectoral exemptions (see Section 4.2.2.).

[452] EDPB Recommendations 01/2020, 2021; see CNIL, Practical Guide, Transfer Impact Assessment, 2025.
[453] EDPB Recommendations 01/2020, 2021, 10-11.
[454] Ibid, 11-13.
[455] Article 45 GDPR; European Commission, Adequacy Decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; accessed on 08.12.2025.
[456] Transfer of data, subject to Chapter V among "groups of undertakings, or groups of enterprises engaged in a joint economic activity" (Article 47(1)(a) GDPR), may be governed by approved binding corporate rules (Article 47 GDPR).
[457] Article 46(2)(c) GDPR; Recital 10 and Annex Commission Implementing Decision (EU) 2021/914.
[458] EDPB Recommendations 01/2020, 2021, 14-21.
[459] Ibid, 14, para. 28.

For the use case, the following specific risks and legal landscape of the importer country must be considered:

- The data shared is considered genetic and health data, qualifying as special category data (Article 9 GDPR) and sensitive personal information (Article 28 PIPL).
- PDX models, as per the latest NHC guidance, are explicitly regulated as HGR material.[460]
- Public authorities in China may access data for national security reasons, potentially undermining SCC safeguards.
- Sectoral implications and thresholds:
    - HGR approval is mandatory for PDX data export.
    - CAC thresholds for security assessments: more than 10k sensitive PI or 1 million non-sensitive PI exported triggers mandatory security assessment.[461]
    - Even if local Chinese rules exempt some data from pre-review, the EU TIA must still assess essential equivalence.
- Residual risk:
    - The risk of lawful access by Chinese authorities is high for PDX data, which is considered strategic and sensitive under Chinese law. If importer countries' laws prevent compliance with SCC, a transfer shall be omitted.[462]
    - The EDPB requires, where no supplementary measures can ensure an essentially equivalent level of protection, the transfer must be avoided, suspended or terminated.

Step 3 concludes that the assessment leads to a high residual risk for the described use case. Where national security assessments and export controls override contractual commitments, SCCs alone cannot guarantee essential equivalence. Without any supplementary measures, a transfer is very likely not in line with the EDPB Recommendations 01/2020 and the outcomes of the Schrems II judgment.

Step 4: Identify and adopt supplementary measures[463]

The focus is on technical, organizational and contractual safeguards. Those measures might include strong encryption, pseudonymization, data minimization and strict contractual (and enforceable) obligations on the Chinese partner regarding onward transfer and data subject rights. If supplementary measures are not effective enough the transfer should not proceed.

---

[460] Q&A on Issues Related to the Management of Human Genetic Resources (Part V), issued 11.10.2025, original: https://www.nhc.gov.cn/qjjys/rlyczygl/202510/f04ebf5bc27a47e5a1ac6f370b3c5ec3.shtml (accessed 01.02.2026), English translation available in Appendix 3.
[461] Article 7 of the Provisions on Promoting and Regulating Cross-border Data Flows.
[462] Recital 19 Commission Implementing Decision (EU) 2021/914.
[463] EDPB Recommendations 01/2020, 2021, 21-23.

For the transfer of genetic and health data to China, the following supplementary measures are required and must be critically assessed for effectiveness:

Technical Measures:

- Strong encryption for data in transit and at rest, with keys held exclusively in the EEA. There must be no possibility of decryption in China and confidential computing should be considered for any data-in-use-scenarios.[464]
- Pseudonymization at source: Remove direct identifiers before transfer and keep keys in the EEA.[465]
- Aggregation: If this is feasible for the foreseen processing purposes, make only statistical or aggregated outputs accessible in China. It shall be ensured not to share raw genetic data in clear text.
- Additional considerations:
    - Non-personal information/anonymous data or non-sensitive personal information of low volume may fall under Chinas exemptions (<100.000 data subjects; FTZ negative list).
    - Local filings may be exempt, but the TIA must document why no personal data is involved or why anonymization is robust.[466]
    - If data is truly anonymized the residual risk is low or conditionally acceptable.

Organizational measures:

- Strict data minimization: Transfer only the minimum necessary data for the given research purpose.[467]
- Access controls and audit logging: Document all access to shared data and maintain audit trails.

Contractual measures:

- SCCs must include clauses prohibiting any onward transfer, ensuring the exporter is notified in case of any access requests by governments and mandating the suspension of the transfer, in case a compliant transfer cannot be ensured.[468]
- The Chinese partner must warrant compliance with HGR approvals, maintain full documentation and notify the EU exporter of any regulatory changes or access requests.

[464] See TeleTrust/ENISA, Guideline "State of the art" in IT security, Technical and organizational measures, 2025, 28-36 and 40-41; EDPB Recommendations 01/2020, 2021, Annex 2.
[465] EDPB Recommendations 01/2020, 2021, para. 85.
[466] See Recital 101 GDPR & EDPB Recommendations 01/2020, 2021.
[467] EDPB Recommendations 01/2020, 2021, para. 137 and 138.
[468] EDPB, Recommendations 01/2020, 2021, 36-41.

Conclusion

While encryption and pseudonymization align with EDPB guidance and are in theory highly effective[469], genetic data still pose a high re-identification risk. Additionally, joint analysis often requires raw data, making full anonymization highly impractical. While data minimization as well as audit trails are strictly necessary, their impact on systematic state access is insufficient. SCC clauses prohibiting onward transfer or mandating the suspension most likely lack enforceability under Chinese jurisdiction. Even with robust safeguards in place, the risk of lawful access by Chinese authorities remains high for genetic data.[470]

10.3. Appendix 3: Translations Chinese sources

10.3.1. Data Security Technology – Rules for Data Classification and Grading

The original Chinese text is available online: https://www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf?mc_cid=b0acb1c7ee&mc_eid=627c47469b

The translation has been conducted using Microsoft 365 Copilot Chat on 18.10.2025.

Chinese	**English**
GB/T 25069—2022**界定的以及下列**术语和定义适用于本文件。	The terms and definitions defined in GB/T 25069—2022 and the following apply to this document.
3.1 **数据** data	3.1 Data
任何以电子或者其他方式对信息的记录。	Any record of information in electronic or other forms.
3.2 **重要数据** key data	3.2 Key Data
特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。	Data in specific domains, groups, regions, or with certain precision and scale, which, if leaked, tampered with, or destroyed, may directly endanger national security, economic operations, social stability, public health, and safety.
注：仅影响组织自身或公民个体的数据一般不作为重要数据。	Note: Data that only affects the organization itself or individual citizens is generally not considered key data.
3.3 **核心数据** core data	3.3 Core Data
对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。	Data with high coverage, precision, scale, or depth in a domain, group, or region, which, if illegally used or shared, may directly affect political security.
注：**核心数据主要包括关系国家安全重点**领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。	Note: Core data mainly includes data related to key areas of national security, the lifeblood of the national economy, important livelihoods, major public interests, and other data determined by relevant national departments.

[469] EDPB, Recommendations 01/2020, 2021, para. 90, Annex 2; TeleTrust/ENISA, Guideline "State of the art" in IT security, Technical and organizational measures, 2025.
[470] Article 28 CBL.

3.4 一般数据 general data	3.4 General Data
核心数据、重要数据之外的其他数据。	Other data not classified as core or key data.
3.5 个人信息 personal information	Any information recorded electronically or otherwise that relates to an identified or identifiable natural person.
3.6 敏感个人信息 sensitive personal information	3.6 Sensitive Personal Information
一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。	Personal information that, if leaked or illegally used, is likely to infringe on the dignity or personal and property safety of a natural person.
3.7 行业领域数据 industry sector data	3.7 Industry Sector Data
在某个行业领域内依法履行工作职责或开展业务活动中收集和产生的数据。	Data collected and generated in the course of performing duties or business activities in a specific industry sector.
3.8 公共数据 public data	3.8 Public Data
各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或提供公共服务过程中收集、产生的数据。	Data collected and generated by government departments, organizations with public management and service functions, and their technical support units, in the course of performing public affairs management or providing public services.
3.9 组织数据 organization data	3.9 Organization Data
组织在自身生产经营活动中收集、产生的不涉及个人信息和公共利益的数据。	Data collected and generated by organizations in their own production and operation activities that do not involve personal information or public interest.
3.10 衍生数据 derived data	3.10 Derived Data
经过统计、关联、挖掘、聚合、去标识化等加工活动而产生的数据。	Data generated through statistical, associative, mining, aggregation, de-identification, or other processing activities.
3.11 数据处理者 data processor	3.11 Data Processor
在数据处理活动中自主决定处理目的、处理方式的组织、个人。	An organization or individual that independently determines the purpose and method of data processing in data processing activities.

Appendix G: Important Data Identification Guide / 附录 G 重要数据识别指南

Chinese	**English**
附录 G（规范性） 重要数据识别指南	Appendix G (Normative) Important Data Identification Guide
重要数据识别应在符合 6.5 b) 的基础上，考虑如下因素：	Important data identification should be based on compliance with 6.5 b), considering the following factors:
f) 关系我国科技实力、影响我国国际竞争力，或关系出口管制物项，如反映国家科技创新重大成果，或描述我国禁止出口限制出口物项的设计原理、工艺流程、制作方法的数据，以及涉及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告的数据；	f) Relates to China's scientific and technological strength, affects China's international competitiveness, or relates to export control items, such as data reflecting major national scientific and technological achievements, or describing the design principles, process flows, production methods of items prohibited or restricted for export, as well as data involving source code, integrated circuit layouts, technical solutions, important parameters, experimental data, test reports;

n) 反映生物技术研究、开发和应用情况，反映族群特征、遗传信息，关系重大突发传染病、动植物疫情，关系生物实验室安全，或可能被利用制造生物武器、实施生物恐怖袭击，关系外来物种入侵和生物多样性，如重要生物资源数据、微生物耐药基础研究数据；	n) Reflects biotechnology research, development, and application, reflects population characteristics, genetic information, relates to major outbreaks of infectious diseases, animal and plant epidemics, biosafety laboratory safety, or can be used to manufacture biological weapons, carry out bioterrorism, relates to invasive species and biodiversity, such as important biological resource data, basic research data on microbial resistance;

10.3.2. Q&A on Data Export Security Management Policies

The original Chinese text, issued on 09.04.2025, is available online: https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm.

The translation has been conducted using Microsoft 365 Copilot Chat on 18.10.2025.

Chinese	English
数据出境安全管理政策问答（2025年4月） 2025年04月09日 14:00来源： 中国网信网 【打印】【纠错】 国家互联网信息办公室持续加强数据出境安全管理政策宣贯，指导和帮助数据处理者高效合规开展数据出境活动。经对近期收到的咨询问题进行研究，现将一些有代表性的问题和答复公布如下。	Q&A on Data Export Security Management Policies (April 2025) April 9, 2025, 14:00 Source: China CAC [Print][Report Error] The Cyberspace Administration of China (CAC) continues to strengthen the promotion of data export security management policies, guiding and assisting data handlers to efficiently and compliantly carry out data export activities. After studying recent inquiries, some representative questions and answers are published as follows.
1.如何理解中国数据出境安全管理制度设计？	1. How should we understand the design of China's data export security management system?
答：随着数据跨境流动活动的日益频繁，世界上许多国家和地区从本国、本地区实际出发，对数据跨境流动安全管理作了制度性探索，制定出台了一系列法律法规和规则标准。中国建立数据出境安全管理制度，是法律作出的规定。《网络安全法》《数据安全法》《个人信息保护法》在法律层面对数据出境活动作出明确规定。相关规定不是针对所有数据，只限于重要数据和个人信息。对于确需出境的重要数据，法律作了制度上的安排，经数据出境安全评估认为不会危害国家安全和社会公共利益的，可以出境。对于个人信息出境，法律规定了数据出境安全评估、个人信息保护认证、个人信息出境标准合同等多种途径。总的来看，中国法律关于数据出境管理的规定，旨在保证在华企业因业务需要的数据跨境安全、自由流动，	A: As cross-border data flows become more frequent, many countries and regions have explored institutional approaches to managing the security of cross-border data flows, issuing a series of laws, regulations, and standards. China's establishment of a data export security management system is mandated by law. The Cybersecurity Law, Data Security Law, and Personal Information Protection Law all provide clear legal requirements for data export activities. These requirements do not apply to all data, but only to important data and personal information. For important data that must be exported, the law provides for a system where, after a security assessment determines that export will not endanger national security or public interests, export is permitted. For personal information exports, the law provides multiple channels, including security assessments, personal information protection certification, and standard contracts for personal information export. Overall, China's legal provisions on data export management aim to ensure the secure and free cross-border flow of data needed for business operations in China,

同时对涉及国家安全和公共政策目标的个人信息和重要数据跨境流动进行必要的监管。对于不涉及个人信息或者重要数据的一般数据可以跨境自由流动，重要数据和达到规定数量的个人信息通过数据出境安全评估后可以依法跨境流动。 落实法律规定，国家互联网信息办公室先后出台实施《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》，发布《关于实施个人信息保护认证的公告》及配套认证规则，明确数据出境安全评估、个人信息出境标准合同、个人信息保护认证等制度的实施路径，会同各地、各部门依法有序开展数据出境安全管理工作。	while providing necessary supervision over the cross-border flow of personal information and important data related to national security and public policy objectives. General data that does not involve personal information or important data can flow freely across borders, while important data and personal information exceeding specified quantities can be exported in accordance with the law after passing a security assessment. To implement these legal requirements, the CAC has successively issued the Measures for Data Export Security Assessment, Measures for Standard Contracts for Personal Information Export, and the Provisions on Promoting and Regulating Cross-Border Data Flows, as well as the Announcement on Implementing Personal Information Protection Certification and supporting certification rules. These clarify the implementation paths for security assessments, standard contracts, and certification, and the CAC works with localities and departments to carry out data export security management in an orderly manner according to law.
2.如何保证不同自贸试验区制定数据出境负面清单标准的一致性？	2. How is consistency ensured in the standards for negative lists for data export formulated by different pilot free trade zones (FTZs)?
答：《促进和规范数据跨境流动规定》明确，自贸试验区可在国家数据分类分级保护制度框架下自行制定数据出境负面清单，经省级网络安全和信息化委员会批准，报国家网信部门、国家数据管理部门备案后实施，负面清单外数据出境将免予申报安全评估、订立标准合同、通过保护认证，是促进和便利自贸试验区数据跨境流动的一项创新举措。负面清单制定过程中将充分征求相关主管部门意见，负面清单备案时国家互联网信息办公室会同国家数据局对清单进行审核，针对同一领域，如果已经有自贸试验区发布负面清单，其余自贸试验区可以参照执行，不再重复制定。上述工作确保负面清单符合国家数据分类分级保护制度要求，保证不同自贸试验区负面清单标准的一致性。	A: The Provisions on Promoting and Regulating Cross-Border Data Flows clarify that FTZs may formulate their own negative lists for data export within the framework of the national data classification and grading protection system. After approval by the provincial cybersecurity and informatization committee and filing with the national CAC and National Data Administration, these lists are implemented. Data not on the negative list is exempt from security assessment, standard contract, and certification requirements—an innovative measure to facilitate cross-border data flows in FTZs. During the formulation of negative lists, opinions from relevant authorities are fully solicited. When filing, the CAC and National Data Administration review the lists. For the same sector, if a negative list has already been issued by one FTZ, others may refer to it without duplicating the process. These measures ensure that negative lists comply with national data classification and grading requirements and guarantee consistency across FTZs.
3.自贸试验区数据出境负面清单适用范围如何覆盖更多领域？	3. How can the scope of FTZ negative lists for data export cover more sectors?
答：落实《促进和规范数据跨境流动规定》，国家互联网信息办公室、国家数据局先后完成天津、北京、海南、上海、浙江等地自贸试验区（港）数据出境负面清单备案，对汽车、医药、零售、民航、再保险、深海业、种业等17	A: In implementing the Provisions on Promoting and Regulating Cross-Border Data Flows, the CAC and National Data Administration have completed the filing of FTZ negative lists for Tianjin, Beijing, Hainan, Shanghai, Zhejiang, and others, promoting cross-border data flows in 17 sectors including automotive, pharmaceuticals,

个领域数据跨境流动发挥促进作用。国家互联网信息办公室会同有关部门正在指导各自贸试验区结合各自产业发展特点制定数据出境负面清单，随着更多负面清单的发布实施，覆盖的领域会越来越宽。关于自贸试验区数据出境负面清单发布实施情况，可以关注国家互联网信息办公室官网（www.cac.gov.cn）和相关地方自贸试验区网站进行了解。	retail, civil aviation, reinsurance, deep-sea industry, and seed industry. The CAC, together with relevant departments, is guiding each FTZ to formulate negative lists based on their industrial development characteristics. As more negative lists are published and implemented, the scope of coverage will expand. For updates on the publication and implementation of FTZ negative lists, please refer to the CAC website (www.cac.gov.cn) and relevant local FTZ websites.
4.如何理解和判断个人信息出境必要性？	4. How should the necessity of personal information export be understood and determined?
答：《个人信息保护法》第六条规定，“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息”；第十九条规定，“除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间”。 根据上述法律规定，判断“必要性”的考量因素包括与处理目的直接相关、对个人权益影响最小、限于实现处理目的的最小范围、保存期限为实现处理目的所必要的最短时间等4方面。落实法律规定，国家互联网信息办公室在开展数据出境安全评估工作中，将充分考量数据处理者申报事项的业务场景和实际需求，对个人信息出境必要性进行评估，评估要点主要包括出境活动本身的必要性、涉及自然人规模的必要性以及出境个人信息数据项范围的必要性等。 数据出境涉及众多行业领域，国家互联网信息办公室会同相关行业主管部门，逐步细化明确具体行业领域的数据出境业务场景以及个人信息出境必要范围，为企业机构数据出境提供更为细化的政策指引。	A: Article 6 of the Personal Information Protection Law stipulates that “the processing of personal information shall have a clear and reasonable purpose, be directly related to the purpose of the processing, and be conducted in a way that minimizes the impact on individual rights and interests. The collection of personal information shall be limited to the minimum scope necessary to achieve the purpose of the processing, and excessive collection of personal information is not permitted.” Article 19 stipulates that “unless otherwise provided by laws and administrative regulations, the retention period of personal information shall be the shortest time necessary to achieve the purpose of the processing.” According to these legal provisions, the factors for determining “necessity” include being directly related to the processing purpose, minimizing the impact on individual rights and interests, being limited to the minimum scope necessary for the purpose, and having the shortest retention period necessary for the purpose. In implementing the law, the CAC will fully consider the business scenarios and actual needs declared by data handlers when conducting data export security assessments, and will evaluate the necessity of personal information export, focusing on the necessity of the export activity itself, the scale of natural persons involved, and the scope of personal information data items exported. As data export involves many industries, the CAC, together with relevant industry authorities, is gradually refining and clarifying the business scenarios and necessary scope of personal information export for specific industries, providing more detailed policy guidance for enterprises and institutions.
5.如何识别重要数据？	5. How is important data identified?
答：根据《网络数据安全管理条例》第六十二条规定，重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，	A: According to Article 62 of the Regulations on Network Data Security Management, important data refers to data in specific fields, groups, or regions, or data that reaches a certain level of precision and scale, which, if tampered with, destroyed, leaked, illegally obtained, or misused,

可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。《数据安全技术 数据分类分级规则》（GB/T 43697-2024）附录G《重要数据识别指南》提出了重要数据识别方法。数据处理者可依据相关法律法规、技术标准等识别申报重要数据。	may directly endanger national security, economic operations, social stability, public health, and safety. Appendix G "Guidelines for Identifying Important Data" of the Data Security Technology Data Classification and Grading Rules (GB/T 43697-2024) provides methods for identifying important data. Data handlers may identify and declare important data based on relevant laws, regulations, and technical standards.
6.重要数据是否意味着不能出境？	6. Does important data mean it cannot be exported?
答：对于确需出境的重要数据，法律作了制度上的安排，经数据出境安全评估认为不会危害国家安全和社会公共利益的，可以出境。截至2025年3月，国家互联网信息办公室共完成数据出境安全评估项目298个，其中，44个申报项目涉及重要数据，评估结果为不通过的7个，不通过率为15.9%；44个申报项目涉及509个重要数据项，评估后准予出境的重要数据项为325个，占申报数据项总数的63.9%。 特别说明的是，《促进和规范数据跨境流动规定》明确，数据处理者按照相关规定申报重要数据，未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。	A: For important data that must be exported, the law provides a system whereby, after a data export security assessment determines that export will not endanger national security or public interests, export is permitted. As of March 2025, the CAC had completed 298 data export security assessment projects, of which 44 involved important data; 7 of these were not approved, a rejection rate of 15.9%. The 44 projects involved 509 important data items, of which 325 were approved for export after assessment, accounting for 63.9% of the total. It is especially noted that the Provisions on Promoting and Regulating Cross-Border Data Flows clarify that if a data handler declares important data in accordance with relevant regulations, but has not been notified or publicly designated as important data by relevant authorities or regions, the data handler does not need to declare it as important data for the data export security assessment.
7.行业技术标准制定过程中如何发挥外资企业的作用？	7. How can foreign-invested enterprises participate in the formulation of industry technical standards?
答：国家互联网信息办公室指导有关专业机构在制定行业技术标准过程中，高度重视并积极鼓励中外企业等各方参与，确保标准制定工作充分考虑国内外相关方需求。一是参与机制公开透明。国家互联网信息办公室指导全国网络安全标准化技术委员会坚持开放合作、广泛参与的原则，面向社会长期公开征集工作组成员单位。委员及下设工作组成员覆盖了一批有代表性的外资企业，其拥有和国内企业机构在标准参与、研讨方面平等的权利义务，作为工作组成员单位的外资企业能够全程参与，可在标准研制各环节充分提出意见和建议。二是标准工作程序公开透明。通过面向社会公开征集标准需求和标准参编单位、就标准草案面向社会公开征求意见等方式，确保各相关方公平公正参与标准制定。	A: The CAC guides relevant professional organizations to attach great importance to and actively encourage the participation of both Chinese and foreign enterprises in the formulation of industry technical standards, ensuring that the needs of all stakeholders are fully considered. First, the participation mechanism is open and transparent. The CAC guides the National Cybersecurity Standardization Technical Committee to adhere to the principles of openness, cooperation, and broad participation, and to publicly solicit working group members from society on a long-term basis. Committee members and working group members include a number of representative foreign-invested enterprises, which have equal rights and obligations with domestic enterprises in participating in and discussing standards. As working group members, foreign-invested enterprises can participate throughout the process and fully express opinions and suggestions at all stages of standard development. Second, the standard-setting process is open and transparent. By publicly soliciting standard requirements and participating units, and by publicly seeking comments on draft

	standards, all stakeholders are ensured fair and just participation in standard formulation.
8.集团公司跨境传输个人信息有无更加便利的渠道？	8. Are there more convenient channels for group companies to transfer personal information across borders?
答：一方面，境内多家子公司如同属一家集团公司且数据出境业务场景相似，可以由集团公司作为申报主体合并申报数据出境安全评估或者备案个人信息出境标准合同，提高数据出境工作效率。另一方面，国家互联网信息办公室正在推动出台个人信息出境保护认证相关管理办法，指导第三方专业认证机构对个人信息出境活动进行认证，境内企业和境外接收方任意一方通过认证，企业即可在认证范围内开展个人信息出境活动，对于通过认证的跨国集团，可在集团内开展个人信息出境活动，无需分别与各国子公司单独签订个人信息出境标准合同。	A: On one hand, if multiple domestic subsidiaries belong to the same group company and have similar data export business scenarios, the group company can act as the applicant to submit a consolidated application for data export security assessment or file standard contracts for personal information export, thereby improving the efficiency of data export work. On the other hand, the CAC is promoting the introduction of management measures for personal information export protection certification, guiding third-party professional certification bodies to certify personal information export activities. If either the domestic enterprise or the overseas recipient passes the certification, the enterprise can carry out personal information export activities within the scope of the certification. For certified multinational groups, personal information export activities can be conducted within the group without the need to sign separate standard contracts for personal information export with each foreign subsidiary.
9.申请延长数据出境安全评估结果有效期有无具体流程？	9. Is there a specific process for applying to extend the validity period of data export security assessment results?
答：《促进和规范数据跨境流动规定》将数据出境安全评估结果有效期由原来的2年延长至3年，同时明确有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前60个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请，经国家网信部门批准，可以延长评估结果有效期3年。目前，国家互联网信息办公室正在积极听取各方意见，加快研究延长评估结果有效期的流程，计划通过修订发布相关政策文件的方式予以明确，为企业机构数据出境创造更为便利的条件。	A: The Provisions on Promoting and Regulating Cross-Border Data Flows extend the validity period of data export security assessment results from the original 2 years to 3 years. They also clarify that if the validity period expires and it is necessary to continue data export activities, and there are no circumstances requiring a new data export security assessment, the data handler may, within 60 working days before the expiration of the validity period, apply to the national CAC through the local provincial CAC to extend the validity period of the assessment result. Upon approval by the national CAC, the validity period can be extended for another 3 years. At present, the CAC is actively soliciting opinions from all parties and accelerating research on the process for extending the validity period, planning to clarify it through revised policy documents, thereby creating more convenient conditions for data export by enterprises and institutions.

10.3.3. Q&A on Data Outbound Security Management Policy

The original Chinese text, issued on 31.10.2025, is available online: https://www.cac.gov.cn/2025-10/31/c_1763633376984070.htm

The translation has been conducted using www.deepl.com/de/translator on 21.12.2025.

Chinese	English
5.《**数据出境安全**评估申报指南（**第三版**）》**中**“**数据**处理者收集和产生的数据存储在境内，**境外的机构、**组织或者个人可以查询、调取、下载、导出”**的“境外”是指什么？** **答**：“**数据**处理者收集和产生的数据存储在境内，**境外的机构、**组织或者个人可以查询、调取、下载、导出”**的“境外”是指数据**访问或调用行为发生在境外。境外机构、组织的工作人员在境内查询、调取、下载、导出调用数据处理者存储在境内的数据、没有将数据传输至境外，**不属于数据出境活**动。	5. What does “overseas” refer to in the phrase “Data processors collect and generate data stored domestically, while overseas institutions, organizations, or individuals may query, retrieve, download, or export such data” within the “Data Outbound Security Assessment Declaration Guidelines (Third Edition)”? Answer: The term “overseas” in the statement “Data collected and generated by data processors is stored within China. Overseas institutions, organizations, or individuals may query, retrieve, download, or export such data” refers to data access or retrieval activities occurring outside of China. When personnel from overseas institutions or organizations query, retrieve, download, or export data stored within China by data processors while physically located within China—without transferring the data overseas—such actions do not constitute data transfer activities.

10.3.4. FAQ regarding Human Genetic Resource Management

The original Chinese text is available online: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/39a747744f2242068fdaf39b0452e11e.shtml

The translation has been conducted using https://www.deepl.com/de/translator on 30.12.2025.

Chinese	English
一、采集、保藏行政许可 1.长期大规模队列研究是否需要同时申报采集许可和保藏许可？ **答**：**不需要。有具体研究目的的**项目申报采集即可，但样本如需长期存放则应存储于获批的保藏库。	I. Collection and Storage Administrative Permits 1. Is it necessary to apply for both collection and storage permits simultaneously for long-term, large-scale cohort studies? Answer: No. Projects with specific research objectives need only apply for collection permits. However, if samples require long-term storage, they must be housed in an approved storage facility.
2.**使用已**获批保藏许可内的人类遗传资源，是否还需要申报采集许可？ **答**：**不需要。**	2. When using human genetic resources covered by an approved preservation permit, is it still necessary to apply for a collection permit? Answer: No.
3.对于同时符合采集许可和国际科学研究合作许可/**国**际合作临床试验备案范围的项目，应如何申请？	3. How should projects that simultaneously fall under the scope of both data collection permits and international scientific research cooperation permits/international cooperative clinical trial filings be applied for?

答：仅申报国际科学研究合作许可/国际合作临床试验备案即可。	Answer: Only an application for an international scientific research cooperation permit/international cooperative clinical trial filing is required.
4.已获批采集或保藏许可如发生事项名称变更，应如何申请？ 答：根据《人类遗传资源管理条例实施细则》第四十四条、四十五条要求，对于采集、保藏许可事项名称变更的按照重大事项变更流程进行申请。	4. How should one apply for a change in the name of an approved collection or preservation permit? Answer: According to Articles 44 and 45 of the Implementation Rules for the Regulations on the Administration of Human Genetic Resources, applications for changes to the name of a collection or preservation permit must follow the procedures for major changes.
5.申请采集样本量是否需要与研究方案内容保持一致？ 答：需要。若不一致，则需作出相关合理说明，明确不一致原因。	5. Does the sample size requested for collection need to align with the research protocol? Answer: Yes. If there is a discrepancy, a reasonable explanation must be provided, clearly stating the reasons for the inconsistency.
6.在采集许可申请获得同意后，参与医疗卫生机构是否需要提交伦理审查批件和承诺书至国家卫生健康委？ 答：参与医疗卫生机构在采集活动获得许可后，将本单位伦理审查批件或认可已获批采集许可单位所提供伦理审查批件的证明材料以及本单位出具的承诺书提交至国家卫生健康委，即可开展采集。	6. After obtaining approval for the collection permit application, do participating healthcare institutions need to submit ethical review approval documents and a letter of commitment to the National Health Commission? Answer: After receiving permission for the collection activity, participating healthcare institutions may submit the following materials to the National Health Commission: their own ethical review approval documents, or proof of recognition of ethical review approval documents provided by the approved collection permit holder, along with a letter of commitment issued by the institution. Upon submission, they may proceed with the collection.
二、国际合作行政许可与备案	II. Administrative Licensing and Filing for International Cooperation
1.国际合作剩余样本应如何处理？ 答：对于仍有研究价值的剩余样本，原则上可返还人类遗传资源样本提供方；或按照申报时提交的暂存地点和时间暂存一定期限后，按相关规范予以销毁。	1. How should residual samples from international collaborations be handled? Answer: Residual samples retaining research value may, in principle, be returned to the provider of the human genetic resources. Alternatively, they may be temporarily stored at the location and for the duration specified in the original declaration, after which they shall be destroyed in accordance with relevant regulations.
2.临床试验中，申办方、合同研究组织等合作各方均为中方单位，只有EDC供应商是外方单位，是否需要申请国际合作？ 答：不需要。	2. In a clinical trial where all collaborating parties—including the sponsor and contract research organization—are Chinese entities, and only the EDC vendor is a foreign entity, is it necessary to apply for international cooperation? Answer: No.

3.以上市为目的的临床试验申办方是否需要与临床试验的批件、通知书或备案公布材料的申请方保持一致？ 答：需要。如果临床试验申办方与临床试验的批件、通知书或备案公布材料的申请方不一致，在填报国际合作申请书时，需要提交相关协议等证明材料作为附件，明确各自权责。	3. Does the sponsor of a clinical trial intended for market authorization need to be consistent with the applicant listed on the clinical trial approval document, notification, or filing disclosure materials? Answer: Yes. If the sponsor of the clinical trial differs from the applicant listed on the clinical trial approval document, notification, or filing disclosure materials, relevant agreements or supporting documentation must be submitted as attachments when completing the international cooperation application form to clarify respective rights and responsibilities.
4.正在进行的临床试验项目，因合作方单位性质变为外方单位，是否需要申请国际合作？ 答：需要申请国际合作，应先暂停项目，待国际科学研究合作获批或国际合作临床试验备案取得备案号后方可继续开展。	4. For ongoing clinical trial projects where the collaborating institution has changed to a foreign entity, is it necessary to apply for international cooperation? Answer: Yes, an application for international cooperation is required. The project should be suspended first and may only resume after obtaining approval for international scientific research cooperation or securing a filing number for the international cooperative clinical trial.
5.利用我国人类遗传资源开展的科学研究，外方资助但无实质性参与，是否需要申报国际科学研究合作许可/国际合作临床试验备案？ 答：此类科学研究外方无实质性参与，不获取研究相关数据信息，研究成果与外方不共享（如外资制药企业仅为医疗机构的研究者提供临床研究用药或部分研究经费资助而不分享研究成果），则不纳入利用我国人类遗传资源开展的国际合作管理，不需要申报国际科学研究合作许可/国际合作临床试验备案。	5. For scientific research utilizing China's human genetic resources that is funded by foreign entities but without their substantive participation, is it necessary to apply for an International Scientific Research Cooperation Permit or file an International Collaborative Clinical Trial? Answer: Such scientific research, where the foreign party does not substantially participate, does not obtain research-related data or information, and does not share research outcomes with the foreign party (e.g., a foreign pharmaceutical company merely provides clinical trial drugs or partial research funding to investigators at medical institutions without sharing research results), is not subject to the management framework for international cooperation involving China's human genetic resources. Therefore, it does not require application for an International Scientific Research Cooperation Permit or filing for an International Cooperative Clinical Trial.
6.项目已进行国际合作临床试验备案，但因条件改变需转为国际科学研究合作许可，应如何办理？ 答：应当及时暂停备案的国际合作研究内容，申请国际科学研究合作许可时在其他证明材料中上传总结说明，待获得国际科学研究合作许可后再开展相应研究内容。	6. How should one proceed if an international cooperative clinical trial has been filed but needs to be converted to an international scientific research cooperation permit due to changed circumstances? Answer: The filed international cooperative research activities should be promptly suspended. When applying for the international scientific research cooperation permit, submit a summary explanation among other supporting documents. The relevant research activities may resume

	only after the international scientific research cooperation permit is obtained.
7.**既往已**获批的国际科学研究合作项目符合国际合作临床试验备案的，应如何处理？ **答**：仅待项目需要进行变更时，**重新按照**变更后的整体内容办理国际合作临床试验备案。	7. How should previously approved international scientific research collaboration projects that meet the requirements for filing international collaborative clinical trials be handled? Answer: Only when changes to the project are required should the filing for the international collaborative clinical trial be reprocessed based on the revised overall content.
8.**国**际合作中其他单位主要是指哪些单位？ **答**：**国**际合作中其他单位是指申办方、组长单位、合同研究组织、第三方实验室、参与医疗卫生机构以外可接触到管理范围内的人类遗传资源材料或信息进行实质性参与的相关单位。	8. What other entities are primarily referred to in international cooperation? Answer: Other entities in international cooperation refer to organizations that, outside of healthcare institutions, have access to human genetic resources materials or information within their management scope and engage in substantive participation. These include the applicant, the lead organization, contract research organizations, third-party laboratories, and relevant participating entities.
9.**在申**请国际科学研究合作行政许可时，单位性质为外方的合同研究组织、第三方实验室是否需要提供所在国（**地区**）伦理审查证明材料？ **答**：**不需要**。	9. When applying for administrative permits for international scientific research cooperation, do foreign contract research organizations or third-party laboratories need to provide ethical review documentation from their country (region)? Answer: No.
10.**国**际科学研究合作行政许可和国际合作临床试验备案中需要提交的国际合作协议包括哪些？ **答**：**国**际合作协议包括申办方、组长单位、合同研究组织、第三方实验室及其他单位的相关协议，**其中申**请国际科学研究合作行政许可中申办方、组长单位、合同研究组织、第三方实验室需提供相互关联的中文签字盖章协议；**国**际合作临床试验备案中需要全部合作单位（**申**办方、组长单位、合同研究组织、第三方实验室和其他单位）**提供中文**签字盖章版协议。	10. What international cooperation agreements must be submitted for administrative licensing of international scientific research collaborations and filing of international cooperative clinical trials? Answer: International cooperation agreements include relevant agreements between the sponsor, lead institution, contract research organization (CRO), third-party laboratory, and other entities. For the administrative permit application for international scientific research cooperation, the sponsor, lead institution, CRO, and third-party laboratory must provide mutually signed and stamped Chinese-language agreements. For the filing of international cooperative clinical trials, all cooperating entities (sponsor, lead institution, CRO, third-party laboratory, and other entities) must provide signed and stamped Chinese-language agreements.
11.**国**际合作临床试验备案中的分析单位应如何理解？ **答**：**国**际合作临床试验备案中的分析单位是指涉及人类遗传资源基因信息或核酸类生物标志物信息分析处理的单位。	11. How should the term “analytical unit” be interpreted in the filing of internationally collaborative clinical trials? Answer: In the filing of internationally collaborative clinical trials, an analytical unit refers to an entity involved in the analysis and processing of

	genetic information from human genetic resources or nucleic acid-based biomarker information.
12.在国际合作临床试验备案中如果检测、分析和剩余样本处理在境内单位，是否可以将境内检测、分析和剩余样本处理单位相关情况作为临床试验方案附件进行提交？ 答：可以。	12. For international collaborative clinical trials filed domestically, if testing, analysis, and residual sample disposal are conducted by domestic entities, can the relevant information regarding these domestic testing, analysis, and residual sample disposal entities be submitted as an appendix to the clinical trial protocol? Answer: Yes.
三、信息对外提供或开放使用事先报告	III. Prior Reporting for External Provision or Open Access of Information
1.发表文章涉及开放使用人类遗传资源信息的，应何时进行信息备份和事先报告？ 答：按现行管理规定，应在数据信息开放之前。	1. When should information backup and prior reporting be conducted for articles involving the open use of human genetic resource information? Answer: According to current management regulations, this should be done before the data information is made publicly available.
2.利用已公开的人类遗传资源数据，是否需要进行信息备份和事先报告？ 答：不需要。	2. Is it necessary to back up information and submit prior reports when utilizing publicly available human genetic resource data? Answer: No.
3.信息事先报告的存储地点/网址/编码填写有什么要求？ 答：如果事先报告类型为对外提供，对外提供的方式如果选择网络传输则填写传输网址，如果选择实体存储介质则填写接收方地址；如果事先报告类型为开放使用，开放使用的方式如果选择论文发表、论著发表或会议发布则填写期刊、出版社或会议网址，如果选择信息平台共享，则填写平台网址/编码。	3. What are the requirements for filling in the storage location/URL/code for pre-reported information? Answer: If the pre-report type is “external provision,” and the method selected is “network transmission,” enter the transmission URL; if “physical storage medium” is selected, enter the recipient's address. If the pre-report type is “open access,” and the method selected is “publication in a paper, monograph, or conference,” enter the journal, publisher, or conference URL; if “information platform sharing” is selected, enter the platform URL/code.
4.申请信息开放使用的要求有什么变化？ 答：信息开放使用方式分为“开放使用”和“审核同意后开放使用”两种，申请信息开放使用时需明确开放使用方式。若申请方选择“开放使用”方式，待获得登记号后方可开放使用；若申请方选择“审核同意后开放使用”方式，数据使用方需向备份平台提交申请，备份平台审核同意后开放使用，后续申请方、数据使用方、备份平台等有关单位需加强数据风险管理和安全审核。	4. What changes have been made to the requirements for applying to open data for use? Answer: Data opening methods are categorized as “Open Access” and “Open Access Upon Approval.” Applicants must specify the desired access method when applying to open data. If the applicant selects “Open Access,” the data becomes accessible upon obtaining a registration number. If the applicant chooses “Access Granted After Review,” the data user must submit an application to the backup platform. Access is granted only after the backup platform reviews and approves the request. Subsequently, the applicant, data user, backup platform, and other relevant parties must strengthen data risk management and security reviews.

5.在项目实施过程中产生的人类遗传资源信息传输给EDC供应商或数据统计公司等外方单位按照协议中数据管理约定开展相关工作，是否需要进行信息备份和事先报告？ 答：不需要。但是参加合作的EDC供应商或数据统计公司等外方单位若在协议数据管理约定的范围以外使用相关研究数据，则应由合作双方中的中方数据信息所有者申请数据信息对外提供或开放使用事先报告。	5. When human genetic resource information generated during project implementation is transferred to external entities such as EDC providers or data statistics companies to carry out relevant work in accordance with the data management provisions of the agreement, is information backup and prior reporting required? Answer: No. However, if the participating EDC provider, data statistics company, or other external entity uses relevant research data beyond the scope of the data management provisions in the agreement, the Chinese data information owner among the collaborating parties must submit a prior report for the external provision or open access of the data information.
四、其他问题	IV. Other Matters
1.关于尿液、粪便、血清、血浆等材料是否在人类遗传资源管理范围？ 答：人类遗传资源材料包括所有类型细胞、全血、组织/组织切片、精液、脑脊液、胸/腹腔积液、血/骨髓涂片、毛发（带毛囊）等，其他不含细胞的人体分泌物、体液、拭子等无需申报，尿液、粪便、血清、血浆等可能含有极少量脱落、残留或游离细胞或基因的生物样本不再纳入人类遗传资源材料管理范围。	1. Are materials such as urine, feces, serum, and plasma subject to human genetic resource management? Answer: Human genetic resources encompass all types of cells, whole blood, tissue/ tissue sections, semen, cerebrospinal fluid, pleural/peritoneal effusions, blood/bone marrow smears, hair (with follicles), etc. Other human secretions, bodily fluids, swabs, etc., that do not contain cells do not require declaration. Biological samples such as urine, feces, serum, and plasma, which may contain extremely small amounts of shed, residual, or free cells or genes, are no longer included in the scope of human genetic resource materials management.
2.材料出境申请中如仅涉及尿液、粪便、血清或血浆等材料，是否需要申报？ 答：尿液、粪便、血清或血浆不再纳入人类遗传资源材料的管理范围，因此上述材料出境无需进行申报。	2. For applications to export materials that only involve urine, feces, serum, or plasma, is declaration required? Answer: Urine, feces, serum, or plasma are no longer subject to the management scope of human genetic resources materials. Therefore, declaration is not required for the export of such materials.
3.为科学研究采集全血样本，实际检测材料为血清或血浆，应如何填报？ 答：血清、血浆不再纳入人类遗传资源材料管理范围，如血清或血浆是由采集全血处理获得，则按全血进行申报。全血在医疗卫生机构处理为血清或血浆送至检测单位的，且不进行基因、基因组、转录组、表观组及核酸类生物标志物等检测，该检测单位不再纳入第三方实验室管理；采集的全血送至检测单位进行处理获得血清或血浆的，该检测单位仍按第三方实验室管理。	3. How should whole blood samples collected for scientific research be reported when the actual testing material is serum or plasma? Answer: Serum and plasma are no longer subject to human genetic resource material management. If serum or plasma is obtained by processing collected whole blood, it should be reported as whole blood. If whole blood is processed into serum or plasma at a healthcare institution before being sent to a testing facility, and no genetic, genomic, transcriptomic, epigenomic, or nucleic acid biomarker testing is conducted, that testing facility is no longer subject to third-party laboratory management. However, if whole blood collected is sent to a testing facility for processing to obtain serum or plasma,

	that testing facility remains subject to third-party laboratory management.
4.**利用尿液、**粪便、血清或者血浆等材料用于科学研究进行基因、基因组、转录组、表观组及核酸类生物标志物等检测产生的人类遗传资源信息，**是否需要申**报？ **答**：仅在涉及国际合作、信息对外提供或开放使用事项时，**将**检测产生的上述人类遗传资源信息纳入国际科学研究合作许可/**国**际合作临床试验备案、信息对外提供或开放使用事先报告管理。	4. Is reporting required for human genetic resource information generated from testing of genes, genomes, transcriptomes, epigenomes, nucleic acid biomarkers, etc., using materials such as urine, feces, serum, or plasma for scientific research? Answer: Only when involving international cooperation, provision of information to foreign entities, or open access to data shall the aforementioned human genetic resource information generated from testing be subject to the following management: inclusion in international scientific research cooperation permits/international cooperative clinical trial filings, prior reporting requirements for information provision to foreign entities, or open access to data.
5.伦理审查批件项目名称是否需要与人类遗传资源申报项目名称完全一致？ **答**：**需要**。	5. Does the project name on the ethics review approval document need to be identical to the project name declared for human genetic resources? Answer: Yes.
6.**研究方案内容是否需要与合作**协议完全一致？ **答**：**研究方案的内容**应不超出合作协议范围。	6. Does the research proposal need to be fully consistent with the cooperation agreement? Answer: The content of the research proposal should not exceed the scope of the cooperation agreement.
7.**已**获批的项目，**在申**请变更过程中，**是否可以**继续开展该研究，筛选受试者入组？ **答**：对于已获得许可利用中国人类遗传资源开展国际合作涉及变更的，获得变更审批决定前可按照原获批事项开展研究，变更的事项应在获得同意变更审批决定后方可开展。	7. For approved projects undergoing modification applications, may the research continue and subjects be recruited? Answer: For projects already approved to utilize Chinese human genetic resources in international collaborations that involve modifications, research may proceed according to the original approved scope prior to obtaining the modification approval decision. Modified aspects may only be implemented after receiving the approved modification decision.

10.3.5. Q&A on Issues Related to the Management of Human Genetic Resources (Part I)

The original Chinese text is available online, issued on 01.04.2025: https://www.nhc.gov.cn/qjjys/rlyczygl/202504/e9974e2f7a324590947485b74d796b71.shtml.

The translation has been conducted using https://www.deepl.com/de/translator on 02.01.2026.

Chinese	**English**

商业化人源细胞系是否纳入监管? **已去除**样本相关信息、无法追溯至个人的用于生产或科学研究的永生化细胞系，不纳入人类遗传资源监管范围。	Are commercial human cell lines subject to regulation? Immortalized cell lines used for production or scientific research that have had sample-related information removed and cannot be traced back to individuals are not subject to human genetic resource regulation.

10.3.6. Q&A on Issues Related to the Management of Human Genetic Resources (Part II)

The original Chinese text is available online, issued on 09.04.2025: https://www.nhc.gov.cn/qjjys/rlyczygl/202504/17f9863c65c742d4b31ccb745e26082a.shtml.

The translation has been conducted using https://www.deepl.com/de/translator on 02.01.2026.

Chinese	English
肿瘤异种移植模型是否属于人类遗传资源材料? 细胞系来源的小鼠移植模型（Cell-derived Xenograft，CDX）**不属于人**类遗传资源材料；患者肿瘤组织来源的小鼠移植模型（Patient-derived tumor Xenograft，PDX）**属于人**类遗传资源材料。如涉及PDX**模型出境**，应按照相关规定，申报人类遗传资源材料出境行政许可。	Are tumor xenograft models considered human genetic resource materials? Cell-derived xenograft (CDX) mouse models do not constitute human genetic resources materials; patient-derived tumor xenograft (PDX) mouse models derived from patient tumor tissues do constitute human genetic resources materials. If exporting PDX models is involved, an administrative permit for the export of human genetic resources materials must be applied for in accordance with relevant regulations.

10.3.7. Q&A on Issues Related to the Management of Human Genetic Resources (Part V)

The original Chinese text is available online, issued on 11.10.2025: https://www.nhc.gov.cn/qjjys/rlyczygl/202510/f04ebf5bc27a47e5a1ac6f370b3c5ec3.shtml.

The translation has been conducted using https://www.deepl.com/de/translator on 02.01.2026.

Chinese	English
1.人类遗传资源申报数量注意事项。 人类遗传资源行政许可、备案项目中申报的人类遗传资源材料及信息的申报数量，应不多于申请材料中方案及知情同意书写明的数量。	1. Notes on the Quantity of Human Genetic Resources Declared. The quantity of human genetic resources materials and information declared in administrative licensing and filing projects shall not exceed the quantity specified in the application materials' protocols and informed consent forms.

2.延续行政许可或备案有效期的时限要求。 **被**许可人或备案人需要延续行政许可或备案有效期的，应当在有效期限届满三十个工作日前向国家卫生健康委提出申请，逾期将不予受理。	2. Time Limit for Extending the Validity Period of Administrative Permits or Filings. Permit holders or filing entities seeking to extend the validity period of an administrative permit or filing shall submit an application to the National Health Commission at least thirty working days prior to the expiration date. Applications submitted after this deadline will not be accepted.

10.3.8. Administrative Licensing for the Collection of Human Genetic Resources in China Service Guide

The original Chinese text is available online, issued on 20.05.2025: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/3b99b808608240878f866e53ce3a8e36/files/1746832742892_58540.pdf. An overview of all Service Guides is available online: https://www.nhc.gov.cn/qjjys/rlyczygl/202503/3b99b808608240878f866e53ce3a8e36.shtml.

The translation has been conducted using https://www.deepl.com/de/translator on 02.01.2026.

Chinese	**English**
一、适用范围 **本**许可适用于在我国境内开展的中国人类遗传资源采 **集活**动，包括重要遗传家系人类遗传资源采集活动、特定地 **区人**类遗传资源采集活动和用于大规模人群研究且人数大 **于**3000 **例的人**类遗传资源采集活动的规范和管理。所称人 类遗传资源包括人类遗传资源材料和人类遗传资源信息。 **重要**遗传家系是指患有遗传性疾病、具有遗传性特殊体 质或者生理特征的有血缘关系的群体，且该群体中患有遗传 **性疾病、具有**遗传性特殊体质或者生理特征的成员涉及三代 **或者三代以上**，**高血**压、糖尿病、红绿色盲、血友病等常见 **疾病不在此列**。 **特定地区人**类遗传资源是指在隔离或者特殊环境下长 **期生活**，**并具有特殊体**质特征或者在生理特征方面有适应性 **性状**发生的人类遗传资源。特定地区不以是否为少数民族聚 **居区**为划分依据。 **大**规模人群研究且人数大于3000**例的采集活**动包括但 **不限于**队列研究、横断面研究、临床研究、体质学研究等。 为获得相关药品和医疗器械在我国上市许可的临床研究涉 **及的采集**	I. Scope of Application This permit applies to the collection of human genetic resources within China, including the collection of human genetic resources from significant genetic families, specific geographic regions, and large-scale population studies involving more than 3,000 individuals. It governs the standardization and management of such activities. The term “human genetic resources” encompasses both human genetic resource materials and human genetic resource information. Significant genetic families refer to blood-related groups affected by hereditary diseases, possessing hereditary special constitutions, or exhibiting specific physiological characteristics, where members with such conditions span three or more generations. Common diseases such as hypertension, diabetes, red-green color blindness, and hemophilia are excluded. Human genetic resources from specific regions refer to those from populations living long-term in isolated or unique environments, exhibiting distinctive constitutional traits or adaptive physiological characteristics. Specific regions are not defined based on whether they are ethnic minority settlements. Collection activities for large-scale population studies involving over 3,000 subjects include but are not limited to cohort studies, cross-sectional studies, clinical research, and constitutional studies.

活动不在此列，无需申报采集审批。 应当申请行政许可的人类遗传资源保藏活动同时涉及 人类遗传资源采集的，申请人仅需要申请人类遗传资源保藏 1 行政许可，无需另行申请人类遗传资源采集行政许可。 人类遗传资源材料包括所有类型细胞、全血、组织/组织 切片、精液、脑脊液、胸/腹腔积液、血/骨髓涂片、毛发（带 毛囊）等，其他不含细胞的人体分泌物、体液、拭子等无需 申报。 人类遗传资源信息包括基因、基因组、转录组、表观组 及ctDNA等核酸类生物标志物等数据信息，以及与此数据相关的疾病、人种等关联信息，其他不含人类遗传资源基因信 息数据类型无需申报。 为临床诊疗、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等活动需要，对我国人类遗传资源开展采集活动的， 依照相关法律、行政法规规定执行，不在本许可的适用范围 内。	Collection activities conducted for clinical research aimed at obtaining marketing authorization for relevant drugs and medical devices in China are excluded from this requirement and do not require collection approval. Where human genetic resource preservation activities requiring administrative licensing also involve collection, the applicant need only apply for the human genetic resource preservation administrative license and does not need to apply separately for a human genetic resource collection administrative license. Human genetic resource materials include all types of cells, whole blood, tissue/tissue slices, semen, cerebrospinal fluid, pleural/peritoneal effusions, blood/bone marrow smears, hair (with follicles), etc. Other human secretions, bodily fluids, swabs, etc., that do not contain cells do not require reporting. Human genetic resource information includes data such as nucleic acid biomarkers (e.g., genes, genomes, transcriptomes, epigenomes, ctDNA), as well as associated information on diseases, ethnicity, etc. Other data types that do not contain human genetic resource gene information do not require reporting, such as disease and ethnicity. Other data types not containing human genetic resource information do not require declaration. Activities involving the collection of China's human genetic resources for clinical diagnosis and treatment, blood collection and supply services, investigation and prosecution of illegal activities, doping testing, and funeral services shall be conducted in accordance with relevant laws and administrative regulations and are not within the scope of this permit.