Schriftenreihe der TMF

C. Dierks
P. Kircher | C. Husemann
J. Kleinschmidt | M. Haase

Data Privacy in European Medical Research: A Contemporary Legal Opinion

Medizinisch Wissenschaftliche Verlagsgesellschaft

Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

Band 18

Medizinisch Wissenschaftliche Verlagsgesellschaft

Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

Band 18

C. Dierks | P. Kircher | C. Husemann | J. Kleinschmidt | M. Haase

Data Privacy in European Medical Research: A Contemporary Legal Opinion

Medizinisch Wissenschaftliche Verlagsgesellschaft

Authors

Prof. Dr. med. Dr. iur. Christian Dierks
Dierks+Company
Rechtsanwaltsgesellschaft mbH
HELIX HUB
Invalidenstraße 113
10115 Berlin

Dr. iur. Philipp Kircher
hih – health innovation hub
des Bundesministeriums
für Gesundheit
Torstraße 223
10115 Berlin

Charlotte Husemann
Dierks+Company
Rechtsanwaltsgesellschaft mbH
HELIX HUB
Invalidenstraße 113
10115 Berlin

Julia Kleinschmidt
Mazars Rechtsanwaltsgesellschaft
mbH
Alt-Moabit 2
10557 Berlin

Dr. jur. Martin Haase, LL.M., LL.M.
Dierks+Company
Rechtsanwaltsgesellschaft mbH
HELIX HUB
Invalidenstraße 113
10115 Berlin

Editors
This book was written in collaboration with Thomas Bahls, Dr. Martin Bialke, Prof. Dr. Wolfgang Hoffmann, Henriette Rau and Dana Stahl (University Medicine Greifswald).

MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG
Unterbaumstr. 4
10117 Berlin
www.mwv-berlin.de

ISBN 978-3-95466-603-4 (eBook: PDF)

Bibliographic Information of the German National Library
The German National Library (Deutsche Nationalbibliothek) has listed this publication in its German National Bibliography. Detailed bibliographic information is available online at http://dnb.d-nb.de

Product/Project Management: Anna-Lena Spies, Berlin
Layout & typesetting: zweiband.media, Agentur für Mediengestaltung und -produktion GmbH, Berlin

Please address all comments and criticism to:
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG, Unterbaumstr. 4, 10117 Berlin, lektorat@mwv-berlin.de

Editorial der TMF

Die wissenschaftliche Nutzung von Daten und Biomaterialien erfolgt zunehmend in internationaler Zusammenarbeit. Eine eingehende Auseinandersetzung mit den transnationalen gesetzlichen und datenschutzrechtlichen Rahmenbedingungen ihrer Arbeit ist daher für Wissenschaftlerinnen und Wissenschaftler wichtig, um auch in internationalen Kooperationen Forschungsprojekte rechtssicher durchführen zu können.

Aus diesem Grund freut sich die TMF sehr, ihre bisherigen Gutachten zu datenschutzrechtlichen Fragen um eine europäische Betrachtung der Thematik erweitern zu können. Der vorliegende umfassende Leitfaden trägt zur Klärung bei, wie Datenverarbeitung nach Inkrafttreten der EU-DSGVO im Jahr 2018 in internationalen Kooperationsprojekten in der medizinischen Forschung ausgestaltet sein muss. Er wird damit vielen Wissenschaftlerinnen und Wissenschaftlern eine große Hilfe sein.

Die TMF dankt dem Institut für Community Medicine der Universitätsmedizin Greifswald, namentlich Prof. Dr. Wolfgang Hoffmann und seinen Mitarbeiterinnen und Mitarbeitern (Thomas Bahls, Dr. Martin Bialke, Dana Stahl, Henriette Rau) für die Initiierung dieses Gutachtens im Zuge zweier Projekte, des Baltic Fracture Competence Centres (BFCC) und des Deutschen Zentrums für Herz-Kreislauf-Forschung e.V. (DZHK) – Unabhängige Treuhandstelle Greifswald (THS).

Besonderer Dank gebührt den Autoren des Gutachtens, Prof. Dr. Dr. Christian Dierks und Dr. Philipp Kircher sowie Charlotte Husemann, Julia Kleinschmidt und Dr. Martin Haase.

Ein weiterer Dank geht an die Mitarbeiterinnen der TMF, Valérie Kempter und Sophie Rybczak, für ihre Begleitung der Veröffentlichung des Gutachtens.

Für die TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. im Auftrag des Vorstands

Sebastian Claudius Semler
(Geschäftsführer)

Prof. Dr. Michael Krawczak
(Vorstandsvorsitzender)

Editorial by TMF

The scientific use of medical data and of biospecimen is increasingly proceeding in the form of international collaborations. An in-depth consideration of the transnational legal and data protection framework of their work is therefore important for medical scientists to be able to carry out international collaborative research projects with legal certainty.

Thus, the TMF was more than happy to extend its range of legal opinion papers and expert reports on data protection issues by a volume taking a decidedly European perspective. The comprehensive guidelines developed therein serve to clarify how data processing in international medical research projects should be planned and implemented so as to comply with the EU GDPR, which came into force in 2018. In this regard, the report will be most helpful to many scientists in practice.

The TMF is grateful to the Institute for Community Medicine at University Medicine Greifswald, namely Professor Wolfgang Hoffmann and his colleagues (Thomas Bahls, Dr. Martin Bialke, Dana Stahl and Henriette Rau) for initiating the report in connection with the Baltic Fracture Competence Centre (BFCC) and The German Centre for Cardiovascular Research (DZHK)—Independent Trusted Third Party Greifswald (TTP).

Great thanks are particularly due to the authors of the report, Professor Christian Dierks and Dr. Philip Kircher, as well as to Charlotte Husemann, Julia Kleinschmidt and Dr. Martin Haase.

The TMF also thanks their staff members, Valérie Kempter and Sophie Rybczak, for accompanying the publication process.

For the TMF—Technology, Methods, and Infrastructure for Networked Medical Research on behalf of the board

Sebastian Claudius Semler
(Executive director)

Professor Michael Krawczak
(Chairman of the board of directors)

Preface from the editors

Background

The EU General Data Protection Regulation (GDPR) became effective on May 25, 2018. Its intent is to harmonise and simplify the wide range of data protection frameworks existing to date throughout the EU countries. Opening clauses grant national scope for interpretation and detailing of the new legislation. National data protection law, such as the BDSG-Neu in Germany, was updated since then. A similar process applies to all countries throughout the EU.

International, national, and state-level law must be considered when conducting scientific studies in the medical field, setting up registers or establishing research infrastructures. Complying with the prevailing heterogeneity of pertinent regulation can be challenge, particularly in collaborative medical research settings involving institutions in more than one country. A significant level of uncertainty exists in the scientific community with regards to the interpretation and application of the new legislation when processing medical data for research purposes.

Is data processing that complied with the former regulations automatically compliant with the GDPR regulations? Do I need to check data processing in existing projects against the GDPR regulations again? What measures can I apply legitimately to balance traceability and reproducibility (Good Scientific Practice) with data subject's rights for information disclosure, their right to be forgotten, and privacy by design? Or, more simply: What is allowed, and what is not?

The Institute for Community Medicine of the University Medicine Greifswald implemented several large-scale collaborative data management projects and always did this, of course, compliantly with data protection regulations. For example, the NAKO health study and the DZHK (German Centre for Cardiovascular Research) have implemented the informational separation of powers recommended by the TMF data protection guidelines by establishing an independent Trusted Third Party (TTP). This TTP accepted responsibility for managing patient lists (i.e., record linkage and identity management), providing pseudonyms and, importantly, managing study participant's consents and withdrawals.

In view of this long-standing experience in the data protection sensitive processing of research data, the Institute for Community Medicine has developed a comprehensive catalogue of questions, which summarize different aspects of research data processing, considering the new data protection legislations.

- Part I of the catalogue of questions compiles essential organisational aspects of an EU-wide data management with regard to the GDPR and country-specific aspects in particular, for selected EU countries.

- Part II of the catalogue provides further details of this assessment with regard to the technical implementation of the data protection requirements (including transparency, the right to be forgotten, obligation to inform patients, informed consent, establishment of a data protection management system, privacy by design, technical and organizational measures).

Objective of the Legal Report

In order to answer these questions adequately from a legal point of view and to better support national and international cooperation projects in the future, the Institute for Community Medicine has commissioned the preparation of a legal opinion in mid-2017.

Two specific research projects were selected as use cases to transform the catalogue of questions into legal assessments and advice. The concept of the TTP as data processing entity was to be assessed as well. The two specific research projects are

- The Baltic Fracture Competence Centre (BFCC), an EU-wide register for the collection of fracture data in the Baltic Sea Region funded by the Interreg Baltic Sea Region Programme 2014–2020 (grant number: #R001)
- The German Centre for Cardiovascular Research (DZHK), particularly the TTP part of the scientific data processing infrastructure (MDC grant numbers 81X1400101 [2013–2018] and 81X1400108 [2019–2023])

The legal report provides a "checklist" to validate "data protection compliance" of technical and organisational measures regarding GDPR as well as national regulations for current and future cooperative medical research projects. The necessary financial resources were provided by the BFCC and the DZHK-TTP projects.

Authors of the legal opinion

The law-firm "Dierks + Company" was commissioned by the University Medicine Greifswald to prepare the legal opinion. Dierks + Company is an innovation consultancy for healthcare and life sciences. Prof. Dr. Dr. Dierks is a proven expert in the field of data protection in medical research. He has already prepared numerous legal opinions on behalf of the TMF (Anforderungskatalog Datentreuhänderdienst 2007, Rechtsgutachten elektronische Datentreuhänderschaft 2008, Rechtsgutachten Pseudonymisierung 2007, Rechtsgutachten Datenschutz in der medizinischen Forschung 2009) and is the author of a permanent data protection column at E-Health.com.

A practice-oriented reference on the EU GDPR with numerous application recommendations

As a result, a comprehensive and detailed legal reference work has been developed, which offers high added value, especially for collaborative data management in research projects. The legal opinion sheds light on a multitude of aspects of how to process data in conformity with data protection law in an independent Trusted Third Party, and emphasises the importance of legitimising methods and tools used in daily practice. In particular, the legal opinion provides information on implementation options for highly topical data protection aspects (amongst others) such as:

- Data Transfer across EU countries
- Erasure of person-identifying data
- Right to be forgotten
- Consent requirements
- Legal consequences of withdrawals
- Quality assurance
- Privacy by design

Acknowledgement

On behalf of the Institute for Community Medicine, I would like to thank the authors of the legal opinion Dr. Philip Kircher and Prof. Christian Dierks, as well as Mrs. Charlotte Husemann, Mrs. Julia Kleinschmidt and Dr. Martin Haase. In countless telephone calls with my esteemed colleagues Mr. Thomas Bahls, Dr. Martin Bialke, Mrs. Dana Stahl and Ms. Henriette Rau, they discussed, analysed, and finally clarified even more countless technical as well as organizational details in manifold data management settings. We all hope we have contributed to a European framework for research data management and that this report will clarify, advise and enable researchers and support high quality cooperative medical research on a European scale.

Prof. Dr. Wolfgang Hoffmann
PI of the BFCC and the DZHK-TTP and TMF Board Member

Preface from the authors

The present work is dedicated to the challenges of data protection law in networked research with cross-border implications. It is the result of two legal opinions prepared by Dierks + Company Rechtsanwaltsgesellschaft mbH in close cooperation with Universitätsmedizin Greifswald (UMG) and its Independent Trusted Third Party (TTP). Part I of the legal opinions was prepared on the occasion of the development of a fracture register in the Baltic region, the so-called Baltic Fracture Competence Center (BFCC). Part II subsequently followed in the course of adapting the TTP's processes to the new data protection requirements under the General Data Protection Regulation (GDPR) at the German Centre for Cardiovascular Research (DZHK).

Part I of the legal opinion focuses on the questions of the legal admissibility of data processing and the related questions of the organisation. It was prepared in spring 2018.

Part II of the legal opinion is devoted to more detailed questions regarding the implementation of data protection requirements using the DZHK as an example, in particular concerning special technical and organisational aspects that are particularly relevant in practice. It was prepared between December 2018 and March 2019.

After the completion of Part II, updates to Part I were made selectively where the legal situation subsequently changed.

It should be noted that the reform of European data protection law is still ongoing and that many issues are controversial both in the legal literature and among data protection supervisory authorities. There is hardly any case law on the new legal situation so far.

In addition, other areas of law relevant to medical research are currently undergoing radical change. For example, the regulatory regimes for clinical trials of medicinal products and medical devices are being revised. In this area, too, the law of the member states is changing in addition to the law of the European Union. There are different transition periods, some of which are subject to conditions.

Within the complex framework of research data protection law, it will therefore be of central importance in the coming years to monitor current legal developments.

The authors are admitted as lawyers in Germany. It was therefore not possible to provide information on national law in other Member States. In order to nevertheless gain insight into the law of other EU member states, legal opinions were obtained from partner law firms in the respective countries on certain questions. These opinions were subsequently summarised by the authors in order to provide a first impression of the legal situation abroad.

Prof. Dr. med. Dr. iur. Christian Dierks
Dierks + Company Rechtsanwaltsgesellschaft mbH HELIX HUB

Table of Contents

Part I of the legal opinions: Lawfulness of Processing

FACTS

The University Medicine of Greifswald aims to support the creation of a "Baltic Fracture Competence Centre" (BFCC) to establish a comprehensive fracture register for the Baltic Sea region in Sweden, Finland, Lithuania, Poland, Estonia and Germany with numerous locations in hospitals in these countries. The register will be operated by the University Medicine Greifswald (UMG) in Mecklenburg Western Pomerania, Germany.

The data will initially be used to conduct three research pilots. The research questions relate to:

- post-operative complications
- diagnosis of osteoporosis
- infections

However, the long-term goal is to improve the treatment of fractures.

For the establishment of this register, the existing register in Sweden serves as a model. The data of the Swedish register was collected under Swedish data protection law for quality assurance purposes (tax number as identifier, opt-out consent). The data collected in Sweden is eventually migrated to the central register in Mecklenburg Western Pomerania. New research data from the remaining countries shall be collected in the respective treatment facilities and transmitted to the German registry after explicit consent of the patient has been obtained. In Germany, the required data is collected in hospitals.

The data is collected and immediately pseudonymised. However, the pseudonyms allow a conclusion on the country of origin. Polish records have already been pseudonymised. A recalculation from the pseudonym to the initial value is not possible. However, a de-pseudonymisation can take place in an individual case via the Trusted Third Party involved, if, for example, this should be necessary for medical reasons to adapt the treatment of a particular patient, e.g. if there are random findings relevant to the treatment..

The Trusted Third Party is legally governed by the University Medicine Greifswald but operates independently in organisational, technical and personnel terms. The pseudonymisation is based on concepts of the MOSAIC project[1].

An assessment of the legal situation in Germany and in the respective EU member states should take place. As the project does not run in the respective member states until the European Data Protection General Regulation (GDPR) and the relevant adaptation legislation have been validated, the currently applicable law should be considered in addition to the future legal situation.

This first part of the legal opinion focusses on higher-level legal questions concerning mainly the admissibility of data processing (so-called lawfulness of processing).

On the basis of this legal opinion, a questionnaire was drawn up and made available to partner law firms. The answers to the questions are not given in Part 1 of the legal opinion.

Part 1 of the legal opinion contains at the end of many sections boxes which translate the essential statements on the implementation at the TTP.

---

1 Bialke M, Penndorf P, et al. A workflow-driven approach to integrate generic software modules in a Trusted Third Part., Journal of Translational Medicine. 2015; 13(176). https://doi.org/10.1186/s12967-015-0545-6

1 Executive Summary

The University Medicine Greifswald (UMG) is the controller for the processing of the patient data (both medical and identifying data) which is aggregated in the context of the Baltic Fracture Competence Centre. The processing of patient identifying data is carried out by the so-called independent Trusted Third Party (TTP), which is legally a part of the UMG. The TTP acts independently according to comprehensive organizational measures.

Despite the implementation of a pseudonymisation, the data is personal data according to the data protection law. Furthermore, the data qualifies as "data concerning health" and, thus, particularly sensitive data with respect to the data protection law.

In order to avoid the possibility of criminal liability under Section 203 StGB (German criminal code), it is necessary to obtain the participant's consent in the sense of a release from the obligation of medical secrecy. At the same time, it is recommended to obtain the participant's consent in the sense of data protection law. Under these circumstances, the processing of personal data in the context of a registry is not objectionable under data protection law, both in accordance with the General Data Protection Regulation (GDPR), as well as under the applicable state data protection laws and the new Federal Data Protection Act (BDSG).

To comply with requirements according to criminal law, professional code of conduct and data protection law, it would also be possible to rely on a sufficient anonymisation technique. The instrument of consent, on the other hand, is the most appropriate way of respecting the right to informational self-determination.

2 Legal requirements of data collection and migration

2.1 Preliminary note

On 25 May 2016, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of persons and repealing Directive 95/46/EC (General Data Protection Regulation), in short "GDPR", came into force. It will apply from 25 May 2018 in all European Member States. The GDPR supersedes the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of persons).

At the same time, the new Federal Data Protection Act (BDSG) comes into force and replaces the old BDSG in the version of the announcement of 14 January 2003 (BDSG [old version]). In addition, the so-called Social Data Protection Law according to the German Social Code—Book I (SGB I) and the German Social Code—Book X (SGB X) is revisited.

In terms of its applicability, the BDSG continues to differentiate between non-public and public bodies, so that in the public sector, if applicable, the state data protection laws of the respective federal states are to be applied. As the GDPR is a law in the form of an EU regulation, it is directly applicable in each

European member state. Therefore it is to be applied parallel to the BDSG, the state data protection laws and specific data protection laws; however, in the case of a conflict, the GDPR will have to be applied with priority.

As of 25 May 2018, the following regulatory areas are relevant for German data protection law: the GDPR, as well as the BDSG and the state data protection laws. These are supplemented by sector-specific data protection laws.

This report focuses on the new legal situation as of 25 May 2018. The previous legal framework is compared in individual cases in order to present the situation comprehensively.

2.2 Applicability of data protection law

Data protection law objectively applies to the processing of personal data by or on behalf of a so-called "controller" (under German law often referred to as "responsible body").

2.2.1 Controller

Under the GDPR, the term "Responsible body" from Data Protection Directive is replaced by the term "controller" (Art. 4 para. 7 GDPR), which is defined as follows:

> *"(...) the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."*

This refers to the natural person, legal entity or authority as such. The data protection rights and obligations are linked to the controller, so the controller is the norm addressee.

> The University Medicine Greifswald, a body governed by public law, acts as the operator of the transnational fracture registry platform in the context of the Baltic Fracture Competence Centre. Therefore, it is the responsible body or, according to new law, the controller as far as it determines the means and the purpose of the processing of personal data. The Trusted Third Party processes patient identifying data and is legally a part of the University Medicine Greifswald. In the following, only the term *controller* will be used.

2.2.2 Processing of Personal Data

Data protection law is only applicable if personal data are processed. According to Art. 4 No. 1 GDPR personal data is defined 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."*

The relevant data within the Baltic Fracture Competence Centre are, without doubt, to be classified as personal data.

However, data protection law does not apply to **anonymised data**. Anonymised data is the opposite of personal data, as the personal reference has been removed in such a way that it cannot be restored at all, or at least not with the means that would be likely to be used in general (see recital 26 GDPR) because of the cost of doing so because it would require a disproportionate amount of time, money and manpower so that the risk of identification would de facto be negligible.[2]

Pseudonymised data have a special status. A pseudonymisation can lead to an anonymisation, depending on who can uncover the pseudonym. The term pseudonymisation of data in Article 4 No. 5 GDPR[3] is defined as:

> *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*

The "additional information" can also be referred to as the assignment rule: it allows to assign a pseudonymised record to a natural person again. The difference between anonymisation and pseudonymisation can be depicted as follows: In the case of a pseudonymisation, it is assumed that the assignment rule still exists and, therefore, in any case, for the person who has access to the rule, the data record can be related to a natural person with relatively little effort. A pseudonymisation reduces the risks for the rights and interests of the person concerned as the relevant connections can only be made if the assignment rule is known. Nevertheless, it continues to be personal data for those, who know the assignment rule, which is why the data is subject to the GDPR, as well as the BDSG and the state data protection laws. This case is only different, if and only if the assignment rule still exists but cannot be accessed by a third party. The data is to be considered personal data in respect to one

2 Still with regard to the old legal situation and with reference to the statements of the Advocate General: ECJ, C-582/14, ECLI:EU:C:2016:779 — Breyer, marginal 46.

3 See also Section 3 para. 6a BDSG [old version].

body, whereas it appears as non-personal to another body (so-called relativity of the personal reference). The European Court of Justice (ECJ) also has a relative understanding in this sense. The ECJ assumes that the additional knowledge of a third party, that is the knowledge of the assignment rule, also for the ignorant party is attributable in those cases in which the ignorant party has legal means to access the assignment rule.[4]

> The collection of data for the Baltic Fracture Competence Centre is to be pseudonymized according to concepts of the MOSAIC project, whereby the pseudonym allows a conclusion to the country of origin. In principle, it is not possible to restore any initial values from the pseudonym, however, a de-pseudonymization can be carried out in individual cases with the TTP being involved.
>
> It must therefore be noted that personal data are processed within the scope of the Baltic Fracture Competence Centre—despite the pseudonymization.

2.3 Collection of personal data concerning health of patients for the registry in Germany

2.3.1 Introduction

As already stated, as of 25 May 2018, the GDPR primarily governs data protection law in Germany. Due to the numerous exemption clauses in the GDPR, however, the BDSG, the state data protection laws as well as additional sector-specific data protection laws may also apply.

In the following part of the legal opinion; firstly, it will be examined whether data transfers under the GDPR are permissible and to what extent the BDSG-new, the state data protection laws and the social data protection law must be considered. Secondly, the professional and criminal admissibility will be considered.

2.3.2 Admissibility according to GDPR and BDSG

Fundamentals

With regard to the handling of personal data, in the field of data protection law a prohibition with reservation of permission applies; meaning the processing of personal data is only lawful if a statutory provision allows it or the consent of the data subject has been obtained. Accordingly, Art. 6 para. 1 GDPR states that the processing of personal data will for example be lawful if the data subject has consented to the processing for one or more specific purposes. For particularly sensitive data such as data concerning health, stricter requirements apply according to Art. 9 GDPR.

4 ECJ, C-582/14, ECLI:EU:C:2016:779—Breyer.

Art. 4 No. 15 GDPR defines **data concerning health** as

> *"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."*

At first, data concerning health is subject to a preventive ban, as Art. 9 para. 1 GDPR in principle prohibits the processing. However, in accordance with Art. 9 para. 2 GDPR, this does not apply, inter alia, if the data subject has **expressly** consented to the processing of the personal data mentioned for one or more specified purposes, unless, under Union law or the law of the Member States, the prohibition under paragraph 1 cannot be waived by the consent of the data subject (Art. 9 para. 2[a] GDPR).

Since neither German law nor Union law provides a regulation according to which the prohibition under Art. 9 para. 1 GDPR cannot be waived by the consent of the data subject, the effective consent of the person concerned therefore constitutes a sufficient standard of authority for processing data concerning health in Germany.

According to Art. 9 para. 2 lit. j) GDPR data concerning health can be processed, if processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 para. 1 GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The German legislator has made use of this option in Section 27 para. 1 sentence 1 BDSG as follows:

> *"By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research purposes or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data."*

In that respect, the processing of data concerning health would also be permitted for research purposes without the consent of the data subject if processing is necessary for that purpose and the interests of the controller significantly outweighs the data subject's interests in excluding processing.

> Whether the interests of the controller significantly outweigh the data subject's interests and the processing of personal data concerning health therefore is permitted without explicit consent within the scope of the Baltic Fracture Competence Centre can be left open if the respective data-subjects consent is used.

Especially in a transnational context it is advisable to process data on the basis of a consent given explicitly instead of a statutory permission. Otherwise the legal basis may vary depending on the applicable law of each of the respective member states and, thus, lead to legal frictions.

Requirements for an effective declaration of consent

The requirements for an effective declaration of consent arise in particular from Art. 4 No. 11, Art. 7 GDPR. One of the main requirements is that consent must be informed. The scope of the necessary information is not specified in the GDPR. In particular, there are no guidelines on cases, such as consent to the transfer of data to other persons responsible within the scope of the GDPR.

However, further Information obligations are expressly regulated in Art. 12, 13, 14 GDPR. Art. 12 GDPR contains comprehensive information requirements. In particular, these include those according to Art. 13 and 14 GDPR.

According to **Art. 13 GDPR**, the controller must provide the following information **at the time of the collection** or before:

- the **identity and the contact details** of the controller and, where applicable, of the controller's representative;
- the **contact details of the data protection officer**, where applicable;
- the **purposes** of the processing for which the personal data are intended as well as the **legal basis** for the processing;
- where the processing is based on Article 6 para. 1 (f) GDPR, the **legitimate interests** pursued by the controller or by a third party;
- the **recipients** or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a **third country** or international organisation and the existence or absence of an **adequacy decision** by the Commission, or in the case of transfers referred to in Article 46 or 47 GDPR, or Article 49 para. 1 subpara. 2 GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the **period** for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- existence of the **data subjects rights** to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- the **right to lodge a complaint** with a supervisory authority;
- whether the provision of personal data is a **statutory or contractual requirement**, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- the existence of the **right to withdraw consent** at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the existence of automated decision-making processes;
- in the case of planned further processing for another purpose, the information must again be made available in this regard.

Comparable information obligations follow from Art. 14 GDPR where personal data have not been obtained from the data subject. In this case, the following must also be pointed out:

- **Category of personal data**;
- the **source** of the data.

In any case, the information must be provided within a **reasonable period** of time where personal data have not been obtained from the data subject and, if the data is to be used for communication with the data subject, at the latest at the time of the first communication. If a disclosure to another recipient is intended, the information must be provided at the latest at the time of disclosure.

In case of re-use for another purpose, the information must be made available again, respectively.

Excluded from the information requirements of Art. 14 para. 1—4 GDPR are cases in which the data subject already possesses the respective information, the provision of information turns out to be impossible or disproportionately complex, especially if processing for scientific research purposes would be impossible or seriously impaired as a result, the obtaining or disclosure of the data is expressly regulated by law or the personal data is protected by professional secrecy.

If data are used for different research questions, it will usually be assumed that these are different research projects for which the data are to be processed. In this case, consent to "areas" of research may be permissible (so-called "broad consent" in the context of research purposes).

The GDPR no longer requires written form. However, consent relating to the processing of special categories of personal data must be given explicitly (Art. 9 para. 2[a] GDPR). Furthermore, the controller must be able to demonstrate that the consent was obtained (Art. 7 para. 1 GDPR). It is therefore advisable to adhere to the written form.

The consent is withdrawable at any time. The withdrawal is effective for the future, but not for the past. The person concerned must be informed of this circumstance (Art. 7 para. 3, Art. 13 para. 2[c], Art. 14 para. 2 [d] GDPR).

2.3.3 Admissibility of the processing of personal data according to the state data protection acts (LDSG)

Deviating regulations can result from the state data protection law. As an example, the following state data protection laws will be discussed on the occasion of the BFCC project.

Applicability of the State Data Protection Acts (LDSG)

LDSG Mecklenburg Western Pomerania (LDSG M-V)

The LDSG M-V (from 22th of May 2018) applies according to Section 2 para. 1 LDSG M-V to authorities and public institutions and bodies of the state, the municipalities, the offices, the districts as well as for other legal persons under public law subject to the supervision of the state (public bodies). According to Section 2 para. 2 LDSG M-V, legal entities and other associations under private law that perform public administration tasks and in which one or more of the legal entities under public law mentioned in paragraph 1 are involved with an absolute majority of the shares or votes are also considered public bodies.

> As a corporation of public law, the University Medicine Greifswald is a public body within the meaning of Section 2 para. 1 LDSG M-V.

It should be noted that the BDSG is also applicable to public bodies of the Federal States in accordance with Section 2 para. 5 sentence 2 BDSG (Section 27 para. 1 Sentence 1 No. 2 subpara. b) BDSG [old version]); however, on the condition that they participate in competition as public law company, implement the federal law and are not regulated by the data protection of the state law.

It seems questionable how the execution of federal law by the federal states under Art. 83ff. GG (execution as a separate matter or federal order administration) may entrust a public-law company undertaking offering services in competition with other private companies. In addition, all federal states have enacted data protection laws which provide for the applicability of the regulations on non-public bodies to public-law competitors (for example, Section 2 para. 5 LDSG M-V). Thus, Section 2 para. 5 sentence 2 BDSG-new loses its practical scope of application. The LDSG M-V is therefore applicable.

University clinics are organised under public law—it is one of their main tasks to research and teach. On the other hand, like any other hospital operated by a private institution, they treat patients and settle accounts with health insurance companies and statutory health insurances in accordance with the relevant regulations. Regarding municipal hospitals, it is assumed that these are public law competitors. As far as the treatment of patients is concerned, there is there is a strong indication that university hospitals should also be

classified as competitors, as they offer the same services. Therefore, the BDSG would be applicable. However, when it comes to research projects in university hospitals, this assessment is less certain.

> It could well be argued, that the University Medicine Greifswald is not a public-law competition company. Threrefore the permissibility of the data transfers should be assessed in accordance with both the applicable LDSG and the BDSG.

LDSG Schleswig-Holstein (LDSG S-H)

The LDSG S-H is—like the LDSG M-V—also applicable to public bodies (Section 3 para. 1 Sentence 1 LDSG S-H), but contains a reference to the BDSG [old version] for public law competitors (Section 3 para. 2 No. 4 LDSG S-H). It can be referred to the comments on the LDSG M-V.

Permissibility according to LDSG M-V

As already stated, the data protection law is designed as a prohibition with reservation of permission. According to Section 9 para. 1 LDSG M-V, the processing of personal data relating to health without a consent is permitted for a specific research project, if the data subject's legitimate interests are not prejudiced by reason of the nature of the data, their disclosure or the way they are used, or if the public interest served by the research project substantially outweighs the legitimate interests of the data subject and the purpose of the research cannot be achieved by other means.

Section 9 para. 2 LDSG M-V states, that as soon as this is possible according to the research purpose, the data must be modified in such a way that the individual details of personal or factual circumstances can no longer be attributed to a specific or identifiable natural person or it can only be done with a disproportionate expenditure of time, cost and labour. Until then, the features, with which individual details about personal or factual circumstances can be assigned to an identified or identifiable natural person, must be stored separately. They are to be deleted as soon as the purpose of the research allows this.

According to jurisdiction of the BVerfG, research is a process based on scientific autonomy (methodology, systematics, evidence, verifiability, open criticism, willingness to review) for finding insights, their interpretation and their dissemination (BVerfGE 35, 112f.) Scientific research under Section 9 LDSG M-V has to be interpreted in the light of Art. 5 (3) Sentence 1 GG. According to this, "everything that can be regarded as a serious, planned attempt to ascertain the truth in terms of content and form" is scientific research (see Kühling/Buchner/Weichert DS-GVO Art. 9 marginal 128 with reference to BVerfGE 35, 112).

It is possible to outline scientific research based on different criteria and the question of whether a device dedicated to research, for example if a univer-

sity pursues its activity, if certain scientific methods are used or the activity has the goal of gaining new insights. Today, however, it is recognised that the freedom of scholarship is an individual right of freedom (Maunz/Dürig/Scholz GG Art. 5 para. 3 marginal 82) and that the fundamental right is not confined to scientific professions or institutions and the guarantee of the working conditions of professionally operated science. The correctness of the methods and results is not important either, but only if a serious attempt is made to ascertain the truth (BVerfGE 90, 1).

Therefore, the central question is whether novel findings should be obtained, regardless of which institution and by which scientific methods. Accordingly, scientific research includes basic research and contract research in and for industry (Wagner NVwZ 1998, 1235 [1237]) as well as all matters of relevance to science, i.e. also preparatory and organisational measures that make scientific research possible in the first place (Maunz/Dürig/Scholz GG Art. 5 para. 3 marginal 157).

It is also apparent from the recitals of the GDPR that the processing of personal data for scientific research purposes must be interpreted in a broad sense. This will include processing for technical development, demonstration, basic research, applied research and privately funded research (Recital 159 GDPR). In addition, the objective set out in Article 179 AEUV to create a European research area is to be taken into account (Recital 159 DS-GO). Studies carried out in the public interest in the field of public health are also included. Moreover, public interest is not required (HK-DS-GVO/Kampert DS-GVO Art. 9, marginal 52).

> The establishment of the Baltic Fracture Competence Centre as a fracture register is challenging in terms of data protection law against the background of the storage of particularly sensitive data concerning health. Nevertheless, the register is used for the conduct of research pilots and, therefore, for a specific scientific project.

Permissibility according to LDSG Schleswig-Holstein

Regarding the permissibility according to the LDSG S-H there are no special aspects and in this respect reference is made to the comments on permissibility according to the LDSG M-V.

2.3.4 Permissibility of data transfers according to social data protection law (SGB I and SGB X)

Relation of SGB I and SGB X

The first book of the German Social Code (SGB I) determines the general provisions and introduces the individual social benefits and the responsible service

providers. It also provides the general principles, including social secrecy, and the beneficiary's duties to cooperate.

The tenth book of the German Social Code (SGB X) provides the social administration procedures and social data protection law. It also regulates the cooperation of service providers and their relationships with third parties. In addition to the comprehensive regulations on the procedures, a major focus is on social data protection law.

Social data

In the present case, the permissibility of the data transactions does not follow out of the social data protection law according to Section 35 SGB I-new in connection with Section 67ff. SGB X-new, since no social data subject to social secrecy in the sense of Section 67 Abs. 2 S. 1 SGB X-new are available.

The law defines social data as personal data

> *"which are collected, processed or used by a body mentioned in Section 35 of the First Book with regard to its tasks under this Code". (Section 67 para. 1 SGB X [old version] and correspondingly Section 67 para. 3 SGB X).*

Bodies according to Section 35 SGB I-new are essentially the service providers within the meaning of Section 12 SGB I as well as the bodies listed in detail in Section 35 (1) Sentence 4 SGB I-new. This does not include, for example, the service providers of the statutory health insurance. Hospitals, universities and other relevant bodies are therefore not subject to social secrecy and, therefore, do not process social data. Therefore, Sections 67ff. SGB X-new are in principle not applicable to them, which can also be concluded from a decision of the Federal Social Court of 10 December 2008. The court ambiguously stated that billing in the hands of service providers are social data (BSG, judgment of 10.12.2008—B 6 KA 37/07 R, marginal 30). However, in the same judgment, the BSG made it clear that social data protection law should not be applied to medical providers (BSG, judgment of 10.12.2008—B 6 KA 37/07 R, marginal 23).

2.3.5 Criminal and professional permissibility

Section 203 German Criminal Code (StGB)

Doctors and members of other medical professions, who require an education regulated by the state to practice the profession or make use of their professional title, are obliged to secrecy about what they have been entrusted with or become aware of in their capacity as a doctor. Medical secrecy applies both in hospitals as well as in private practice.

Section 203 (1) StGB stipulates that the unauthorised disclosure of sensitive information, namely a secret belonging to the personal sphere of life that has been entrusted to or that has otherwise become known to a person in the capacity of a doctor or a member of another medical profession is to be punished with imprisonment for up to one year or a fine. Members of other medical professions with state-regulated training for example include medical assistants, nurses and medical-technical assistants.

Medical secrecy comprises facts and circumstances that are known only to a limited number of individuals and in whose confidentiality the person concerned has an objective interest, considering his or her particular situation. The courts (OLG Karlsruhe dated August 11, 2006, 14 U 45/04) and the legal literature predominantly assume that there is an interest in secrecy worthy of protection even for the patient's name and the fact that a doctor has been consulted at all. The relevant data are data concerning health (Art. 4 No. 15 GDPR), which fall within the scope of protection of Section 203 StGB.

According to Section 1 para. 2 s. 3 BDSG the obligation to maintain statutory secrecy obligations or professional or special official secrets that are not based on statutory regulations (including the Section 203 StGB) remains unaffected by the Data Protection regulations.

The revised Section 203 StGB that has taken effect on 09 November 2017—Section 203 (3) StGB—introduced a new set of requirements that allow the disclosure of foreign secrets under strict conditions.

According to Section 203 (3) sentence 1 StGB, it does not constitute a disclosure of the facts if the persons subject to confidentiality make secrets accessible to their assistants who work for them or to the persons who work for them in preparation for the profession. Hospital physician's assistants also include hospital administration employees who are directly involved in medical treatment. This applies, for example, to employees involved in collecting patient data for billing purposes. External persons, who are self-employed or are involved in the operation of a third party, do not fall under the term "assistants".

However, Section 203 (3) sentence 2 StGB stipulates that secret bearers may now disclose foreign secrets to other persons, who participate in their professional or official activities, insofar as this is necessary for the use of their services; the same applies to other participating persons if they themselves again make use of the services of other persons, who participate in the professional or official activities of the secret bearers (Section 203 [3] sentence 2 semisentence 2 StGB). Contrary to the prevailing interpretation of the term "assistant", the only aspect that is relevant for the newly introduced category of "other participating person" is that the person concerned participates in the professional or official actions of the person subject to confidentiality without being integrated into their sphere.

Rather, the basis for participation may be a contractual relationship, possibly including multi-level contractual relationships (see Section 203 [3], sentence 2, semisentence 2). Such cooperation shall be deemed to exist where the person concerned is directly involved in the professional activity of the person subject to confidentiality, its preparation, implementation, evaluation and administration. Examples of this are paperwork, accounting, acceptance of telephone calls, file archiving and destruction, installation, operation, maintenance—including remote maintenance—and adaptation of IT equipment, applications and systems of all kinds, provision of IT equipment and systems for the external storage of data and participation in the fulfilment of accounting and tax obligations of the person responsible for professional secrecy.

By mentioning the provision of systems for the external storage of data, the justification for the law explicitly addresses the storage of data of persons subject to confidentiality, such as doctors, in so-called cloud systems. This illustrates the extent to which the legislation reduces the protection of professional secrets.

> Nevertheless, it should be noted that the Baltic Fracture Competence Centre is not to be regarded as a service provider in the sense of a data processor for a hospital and that the employees are therefore not considered to be "other persons" within the meaning of Sec. 203 (3) sentence 2 StGB. A disclosure to the Baltic Fracture Competence Centre is therefore not already authorized by law.

Medical professional code

In addition to the criminal offence of Section 203 StGB, the protection of medical secrecy is also subject to the medical professional codes of the medical associations in the federal states. In Mecklenburg Western Pomerania and Schleswig-Holstein, medical secrecy is regulated identically in wording in Section 9 of the Professional Code of the Medical Association of the Mecklenburg Western Pomerania and Section 9 of the Professional Code of the Medical Association of the Schleswig-Holstein (hereinafter referred to individually or jointly as "BO").

Section 9 (1) and (2) BO essentially repeats the prevailing opinion on the interpretation of Section 203 StGB. Section 9 (3) stipulates that the doctor must inform his employees about the duty of confidentiality and record this in writing.

Section 9 (4) BO regulates an important exemption from medical secrecy if the patient is treated by several doctors (simultaneously or consecutively). In these cases, the doctors should communicate with each other and write medical reports if the patient's consent is available or can be assumed.

Anyone who violates the duty of professional secrecy as a doctor is acting contrary to professional law and may within the framework of the enforcement

of the professional code be sentenced before a professional court with a so called warning, a reprimand, a fine of up to EUR 50,000, a revocation of the active and passive chamber suffrage or to the finding that the accused is unworthy of exercising his profession. In the latter case, this will usually lead to the revocation of the professional license.

Suppression of medical secrecy

Only the unauthorised disclosure of patient secrets is prohibited. To date, four powers of disclosure have been developed in jurisprudence and literature, which enable doctors to legitimately disclose patient secrets: In addition to the express consent of the patient to be treated here, the right of disclosure may also result from a presumed consent of the patient, a statutory right of disclosure or a statutory right of disclosure and from the so-called balancing interest principle by weighting the affected legal interests.

To avoid any criminal liability, it is expressly recommended to obtain a sufficient written release from medical secrecy with regard to the transfer of data to the registry in form of an express consent of the person concerned. Generally, both criminal liability under Section 203 StGB, as well as a violation of Section 9 BO can be thereby eliminated. Although the consent does not have to be obtained in written form, it is particularly recommended with regards to evidential questions.

Intermediate Results

> Patient data relevant to the Baltic Fracture Competence Centre are subject to medical secrecy.

Unauthorised disclosure is a violation of Section 203 StGB and Section 9 BO. Due to the extensive consequences, the consent by each patient must be obtained in the form of a release from the obligation to maintain confidentiality.

2.3.6 Processing

Data protection law makes an exception to the requirement of the consent of the data subject with regard to the transmission of his personal data if a so-called order-data processing or, according to the new law, so-called processing exists. Processors are not considered "third parties" and processing is generally permitted without the need for additional permission.

According to Art. 4 No. 8 GDPR, the term processor is defined as

> *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".*

Characteristic for the processing is a subordination of the processing to the purposes of the controller. Only the controller may dispose of it, while the processor acts independently, but exclusively in accordance to instructions. As soon as the processor determines or may determine the purpose because of deviating individual interests in the data, processing is inevitably ruled out. It must be the person responsible who is held accountable for the processing, which may result from an explicit legal assignment, from an implied competence or from factual influence. Regarding the means of processing, however, a certain scope for concretion on the part of the agent does not rule out processing.

The figure of processing is directly regulated in the GDPR. There is no exemption clause to divergent provisions in Member State law.

The discussion under the old legal situation about the demarcation between order data processing and the so-called transfer of functions is obsolete due to the new regulation of data protection law and the associated legal definition of both the processor and the controller.

If two bodies jointly determine the purpose and the means of processing, this relationship cannot constitute processing because the characteristic feature of subordination is missing (see above). Instead, both bodies are considered joint controllers within the meaning of Art. 26 GDPR.

> Whether and to what extent the hospitals or agencies collecting data for the Baltic Fracture Competence Center are to be regarded as processors cannot be clearly answered and depends on the detailed relationship between the parties involved.

If one assumes that hospitals also pursue their own interest in the collection of personal data, processing should be ruled out (see Beck OK DatenschutzR/ Spoerr, DS-GVO Art. 28, marginal 19).

If processing can be assumed, the hospitals would not be classified as third parties in relation to the registry, so that the patient would not have to give his or her consent to data transfer between these bodies. But furthermore, according to Art. 28 (3) GDPR, a comprehensive contract between the processor and the controller would be required in order to bind him to the specifications of the controller. But even then, the hospital concerned should not transfer patients' data to the registry without the patient's permission, namely a release from medical secrecy.

In this context, it is highly recommended, which is also to be the safest way, to treat the data migrating bodies in relation to the registry not as a processor, but as a third party unbound by instructions, and to obtain the data protection consent in addition to the release from the medical secrecy obligation. It is therefore advisable to set out the relation and independence of all entities involved in order to clarify the legal situation in a cooperation document.

2.3.7 Result

The establishment of the registry is subject to increased requirements due to the processing of data concerning health. Compared to the former legal situation, the new laws contain even stronger protection mechanisms for data concerning health (cf. Art. 9 GDPR and Sec. 22 BDSG-new). The German legislator makes exceptions in the area of scientific research within the framework of the new BDSG. However, in order to avoid criminal liability according to Sec. 203 StGB or sanctions according to Sec. 9 BO, an explicit consent for the data transfer by the person concerned is necessary.

> It is expressly recommended to obtain an explicit consent of the data subject for the processing of data concerning health for collection in the Baltic Fracture Competence Centre and to avoid criminal liability according to Sec. 203 StGB or sanctions according to Sec. 9 BO, since such a consent is in any case a sufficient permission standard.

2.4 Data migration

About the data migration to the registry from the different European Member States to Mecklenburg-Western, Art. 1 (3) GDPR applies, which regulates the free movement of data within the EU as follows:

> *"The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."*

The aim is to ensure that the exchange of personal data throughout Europe remains as free as it would otherwise be within a Member State. This is particularly important for the use of data in different Member States, whether processed directly or by order. In this respect, nothing different applies to data transfers within the EU and, thus, to the data migration about the GDPR relevant here. The statements on this topic made above are thus to be referenced.

Despite the GDPR, which is equally applicable in all EU Member States, divergent national legislation specificities may have to be taken into account when implementing the GDPR. For this purpose, we have prepared a questionnaire to be found in Annex 1, which is answered by our partner law firms in the other EU Member States.

The results of the questionnaire are presented separately.

Part II of the legal opinions: Detailed Questions on organisational and technical measures

FACTS

During the implementation of data processing processes that comply with data protection laws, questions of detail often arise. The present legal opinion is intended to provide both concrete answers and assistance for the independent application of the law in individual cases. The following questions will be answered using the example of cooperation between the “Deutsches Zentrum für Herz-Kreislauf-Forschung e.V.” (DZHK) and the independent Trusted Third Party (TTP) of the University Medicine Greifswald (UMG).

1 Transparency

The principles relating to processing of personal data are set out in Article 5 GDPR. Transparency is one of the main principles of the GDPR.

> *Which technical and organisational measures must be implemented in order to achieve the required level of transparency*[5]*?*
>
> *Is a combination of manual and automatic processes advisable/permissible here (cf. examples GMDS guidelines)?*
>
> *Can the necessary obligation to prove transparency be realised alternatively by a suitable passage in the data protection concept? (e.g. "within the TTP the TTP employee may carry out the processing according to consent")*

According to Article 5 (1) (a) GDPR personal data shall be processed in a transparent manner in relation to the data subject ('transparency'). On the one hand this principle is intended to prevent the clandestine processing of per-

5 Examples are system documentation, rules for applying for, assigning and changing authorizations, logging of: Call of programs, use of automated retrieval procedures, setup of users, call of administration tools, creation of rights profiles, attempts of unauthorized login, import and modification of application software, attempts of exceeding authorizations, changes to file organization, input/change of data, implementation of data backup measures, data transmissions, deletion of data.

sonal data; on the other hand, it leads to comprehensive information obligations of the controller about the processing of data related to the data subject.[6]

Due to recital 39 (second sentence) it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used (recital 39, third sentence). That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed (recital 39, fourth sentence). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing (recital 39, fifth sentence). In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data (recital 39, six sentence).

The principle of transparency does not only include traceability, but also predictability.[7] The whole context of the processing has to be made transparent: information about the controller (who?), quality and quantity (what?), the time (when?), the reason (why?) and the purpose (for what?).[8]

The principle of transparency runs through the whole regulation (cf. Art. 12–15 GDPR). It is mainly taken into account with the information duties according to Art. 13, 14 GDPR. The information mentioned there must be made available to the data subject.

GDPR does not say in which form the information is to be made available. Therefore paper-based information sheets as well as downloading information from a website or for example providing it via smartphone app come into consideration. In order to ensure that the essential information is available in time, it is recommended to hand it over on paper before the first collection of personal data in the context of the consent process and to keep it accessible online for later retrieval.

A mere mention in a data protection concept will as a rule not satisfy these requirements. Rather, it is recommended to attach the required information sheets in their entirety to the data protection concept in addition to the publication in a data protection declaration. The principle of transparency also

6 *Herbst*, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Art. 5, marginal 18.
7 cf. Frenzel, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, DS-GVO, Art. 5, marginal 21.
8 cf. Frenzel, in: Paal/Pauly/Frenzel, DS-GVO BDSG, 2. Auflage 2018, DS-GVO, Art. 5, marginal 21.

implies that certain basic information must be available, in particular before consent is given, in order to be informed. Only informed consent can be legally effective. For this information, it would not be sufficient to refer the consenting party to a website where he could access this information. Rather, this information should be part of a consent form (for the requirements of an informed consent form, see Part I. 2.3.2 "Requirements for an effective declaration of consent" and Part II.5.1 "Informed Consent").

2 Auditing

To document cross-system processes, audit logs are created by different systems.

To what extent may these logs contain general information (for example, nurse A created patient with pseudonym A1B2C3 in system B and stored a consent with date xx.xx.2018)?

May these logs contain personal identifying data such as "Max Müller, date of birth: 21.05.2001)?

May server logs in selected higher log levels for the development and debug process ("service case") such as DEBUG or TRACE contain IDAT for troubleshooting (i.e., log level must be set explicitly, not the normal ones)?

According to our research, there is no legal regulation that specifies in detail what a log file must look like. However, we recommend applying the general data protection principle of data minimisation and balancing it with a legitimate interest in an audit trail.

Accordingly, it would, for example, be permissible to record that a certain change was made by a certain person and, in particular, when this happened. We do not see a compelling necessity to use non-pseudonymous data.

Since personal data must also be erased in log files when a justified request for erasure is made, it is not advisable to work with clear names such as IDAT would contain.

Which data can be retained in the event of a withdrawal of a declaration of consent? What must and can be "masked" practically? Where is the line between data protection and the need for IT and information security?

Data protection and data security are characterised by partially identical objectives. These include the availability and integrity of data. If an erasure claim is justified, the right to informational self-determination prevails in case of a conflict of objectives. Limits of the erasure claim in the sense of the article 17 para. 2 GDPR (right to be forgotten) are to be found under consideration of the available technology and the implementation costs appropriate measures, also of technical kind under consideration of the available technology and the implementation costs appropriate measures, also of technical kind, in order to inform for the data processing responsible persons, who process the personal data, about the fact that a person concerned of them has demanded the erasure of all links to these personal data or of copies or replications of these personal data. In addition, claims for erasure are, inter alia, limited according to Article 17 para. 3 lit. d) GDPR where data is processed for scientific purposes and the enforcement of the claim for erasure is likely to make it impossible or seriously impede the achievement of those purposes.

3 Erasure of Personal Data

3.1 The right to be forgotten

If pseudonyms are generated and assigned to a unique personal identifier (mapping) and this assignment of a PSN-Value relationship is deleted (virtual anonymisation), no more conclusions about the identity of a person can be made within the TTP.

Does this procedure correctly implement the right to be forgotten?

The term "right to be forgotten" is often used without taking into account the differences to the general right to erasure. While the right to erasure is intended to ensure that data is not unlawfully processed by a particular data controller, the right to be forgotten addresses the special constellation of published data that can easily be found on the Internet via search engines worldwide. In its landmark ruling of 13 May 2014 (Google Spain), the European Court of Justice (ECJ) established the right to be forgotten as the right of a data subject to demand the deletion of personal search results (de-listing) from the operator of a search engine under certain conditions on the basis of Art. 7 and 8 Charter of Fundamental Rights of the European Union and from Art. 12 and 14 of the Data Protection Directive.[9] Under the GDPR the 'right to be forgotten'

9 EuGH Urt. v. 13.5.2014 – C-131/12, BeckRS 2014, 80862; ECLI:EU:C:2014:317.

as an aspect of the right to erasure is laid down in Article 17 GDPR which is overwritten with "Right to erasure ('right to be forgotten')".

In a first step Article 17 para. 1 GDPR lists groups of cases in which personal data of the data subject must be erased. As a second step Art. 17 para. 2 GDPR provides: Where the controller **has made the personal data public** and is obliged (pursuant to Art. 17 para. 1 GDPR) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take **reasonable steps**, including technical measures, **to inform controllers** which are processing the personal data that the data subject has requested the erasure by such controllers of any **links to, or copy or replication of, those personal data**. Finally, Article 17 para. 3 GDPR contains exceptions to the obligations set out in paragraphs 1 and 2.

One can say that there is no comprehensive right to be forgotten in the GDPR. There is only a deletion duty according to Article 17 para. 1 GDPR and an information duty towards third parties who process this published data according to Article 17 para. 2 GDPR. The latter is specifically tailored to the online environment (see recital 66). Article 17 para. 2 GDPR precedes the more general regulation of the Article 19 GDPR according to which a general "Notification obligation regarding rectification or erasure of personal data or restriction of processing" exists. Art. 19 GDPR states:

> *"The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17 (1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."*

Considering the above-mentioned remarks, it becomes clear that the question does not concern a case of the "right to be forgotten" in the sense of the obligation to inform, but rather directly concerns the erasure claim according to Article 17 para. 1 GDPR. Under normal circumstances, a TTP will not publish any personal data and, most importantly, will not publish it on the Internet.

The question of the correct implementation of erasure of data and whether the virtual-anonymisation described above can suffice is answered in Part II.6.

3.2 Erasure of Personal Data in backups

> *Data are regularly part of incremental or complete backups or dumps, which are written on tape as a series that partly rotates with a long cycle (years). Backups are generally encrypted. In the case of withdrawals or deletion requests, how do we deal with the fact that it is almost impossible to clean all series and databases in backups? Please develop and suggest a data protection compliant procedure model for this.*

The obligation to erase personal data derives from Article 5 para. 1 lit. a), b), e) GDPR and Art. 17 GDPR. If one of the grounds set out in Article 17 para. 1) GDPR applies, the personal data of the data subject has to be erased by the controller. As a rule data copies that are created during data backup must be taken into account during erasure. If the data is erased in the active system operation, it must also be erased promptly in the backup and in other backup media, regardless of how many backups are available.

However, according to Article 17 para. 3 GDPR the right of erasure of personal data shall not apply to the extent that processing is necessary for

- exercising the right of freedom of expression and information,
- compliance with a legal obligation which requires processing,
- reasons of public interest in the area of public health,
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and
- the establishment, exercise or defence of legal claims.

None of these exceptions apply in the case that is to analyse here and the right of erasure is granted **unconditionally**. Despite that, Article 23 GDPR allows the Member States to enact further restrictions to the right to erasure, which the German legislator made use of in **Section 35 BDSG**. According to this, the data subject shall not have the right to erasure, if in the case of **non-automated data processing** erasure would be impossible or would involve a **disproportionate** effort due to the specific mode of storage **and if the data subject's interest in erasure can be regarded as minimal**. In this case, the controller only has to make sure that the requirements of Article 18 GDPR (restriction of processing) are met. As described in the question, it can very well be argued, that Section 35 BDSG is applicable. Though we have to point out that this Section has been discussed controversially and the National Data Protection Board (Datenschutzkonferenz—DSK) has expressed doubts about the conformity with European law.

We therefore suggest to implement procedures to make sure that the right to erasure can be guaranteed in the future: IT-systems processing personal data should be designed in such a way that individual data sets can be identified and deleted in all redundancies. Since the purpose of a security backup can only be fulfilled if deletions in the active system are not immediately effective in the backup system, a deletion concept should specify the intervals at which deletions also affect backups. In the event of data recovery, data may be restored to systems where it was previously erased. In this case, the data must be erased again immediately. It must also be ensured that the backup copies are only used for system recovery purposes. A concept on erasure should specify the intervals at which deletions are transferred to backups. The concept on erasure should become part of the general data protection concept and include the essential considerations for justifying the design of the erasure process. The person concerned must be informed about the fixed erasure periods according to the obligations under Articles 13, 14 GDPR.

4 Information Duty

According to Art. 13 GDPR, a person must be informed comprehensively about the data collected. Must this be done immediately or is it permissible to wait for a request and provide information within a reasonable period of time (e.g. 4 weeks)?

The duty to inform derives from the principle of transparency in Article 5 (1) (a) GDPR. It is specified in Article 12 et. Seq. GDPR. Two constellations can be distinguished. Either data is collected directly from the data subject or indirectly:

According the wording of Art. 13 GDPR the controller shall provide the data subject **at the time when** personal data are obtained where personal data relating to a data subject are collected **from the data subject**.

According to Art. 14 GDPR the controller shall provide information where personal data **have not been obtained from the data subject** within a **reasonable period** after obtaining the personal data, but at **the latest within one month**, having regard to the specific circumstances in which the personal data are processed (Article 14 para. 2 lit. a) GDPR, if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject (Article 14 para. 2 lit. b) GDPR) or if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed (Article 14 para. 2 lit. c) GDPR.

5 Consent

5.1 Informed Consent

Who can or must conduct an informative talk with the patient in order to guarantee an informed consent? Can this be done by trained personnel (study nurse, receptionist etc.)? Which other conditions must be observed?

General data protection law does not contain any specific requirements for an informative talk.

According to Article 4 no. 11 GDPR Consent of the data subject is defined as:

> *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"*

However, voluntariness presupposes that the essential information of the data subject is available and that the information has been understood. Irrespective of the legal capacity, the ability to give consent must be determined on the basis of whether the person concerned is capable of understanding and is therefore in a position to understand the consequences of an encroachment on his or her right to informational self-determination made possible by the consent.

Where possible, a distinction should be made as to which legally protected right consent refers to. Consents are required by different legal norms, but may contain different declarations which may relate to different legal interests. Consent according to Article 6a) GDPR or Article 9 Section 2a) GDPR is judged according to the standards of Article 7 and 8 GDPR. It accordingly does not explicitly require an informative talk, this is to be judged differently with consents which are supposed to allow an intervention into the physical integrity, e.g. for an invasive examination. If an invasive examination and data processing are required to participate in a study, which both are to be legitimised by consent, there would be two separate declarations of the patient. In some laws, however, these distinctions become blurred. For example, Section 40 (1) Sentence 3 no. 3c) German Medicines Act (AMG) requires that the consent with regard to participation in a clinical trial must also expressly refer to the collection and processing of information on health. In an international context, a uniform English-speaking and quality-assured consent may be preferred. However, since it cannot be assumed that every study participant speaks English, the consent form in English should be available in the respective national language.

Informed consent in the sense of data protection law can already be achieved solely on the basis of written information provided, without an informing person. However, in order to ensure that questions can be answered competently and that the patients ability to give consent can be ensured, it is always recommended that a sufficiently qualified person be available to provide the information. Specific certificates of specialist knowledge are not required.

Depending on the type of research project, however, **sector-specific regulations may result in different requirements**. For example when it comes to clinical trials of a medicinal product, Section 40 para. 2 of the Medicinal Products Act (Arzneimittelgesetz—AMG) states:

> *"The person concerned shall be informed by an investigator who is a physician, or in the case of a dental trial, a dentist, or by a member of the investigating team who is a doctor, or in the case of a dental trial, a dentist about the nature, significance, risks and implications of the clinical trial as well as about his/her right to withdraw from the clinical trial at any time; a generally comprehensible information sheet is to be handed out to him. Furthermore, the person concerned is to be given the opportunity to have a counselling session with an investigator or a member of the investigating team who is a doctor, or in the case of a dental trial, a dentist about the other conditions surrounding the conduct of the clinical trial."*

Since the AMG does not make a clear distinction between consent to data processing and consent to participation in a clinical trial, the safest way would be to also provide the information required under data protection law as a part of the informative talk required under Section 40 para. 2 AMG.

Similar requirements can be found, for example, in Section 20 para. 1 sentence 4 no. 2, papa. 4) no. 4 and Section 21 no. 3 of the Medical Devices Act (Medizinproduktegesetz—MPG).

Is a (supplementary) country-specific consent advisable here?

A country-specific consent would only be advisable if there are country-specific requirements that differ from each other.

Is the TTP obliged to validate the linguistic correctness e.g. of Lithuanian, Polish or Estonian consents?

Does the TTP have to be able to assure the quality of these consents and guarantee their correctness? Only in this case, the TTP may be able to validate/check the consents and handle or correct errors.

The TTP would only be obliged to check the correctness if the TTP would appear for the processing as controller in the sense of the Article 4 no. 7 GDPR and an ineffectiveness of the consent could result from the linguistic incorrectness. The GDPR does not expressly stipulate a duty to validate, but the data controller must ensure the lawfulness of the processing of personal data (Article 5 Section 2 GDPR).

If the TTP acts as a processor, it shall not be obliged to examine the legality of the contract. If the processor has doubts as to the lawfulness of data processing, he should inform the controller accordingly.

If the TTP is part of the legal entity of the controller, it would be part of the controller and thus would have to ensure the lawfulness of the processing of personal data.

According to the GDPR, consent can be given by electronic means. Does this officially allow the sole use of digital signatures? (i.e. no paper-based consensus is obtained, the signature is recorded and stored directly electronically). Are both of the following option of the electronic signature permitted?

Option 1: Capture via tablet PC and only the signature in reproducible form.

Option 2: Capture via SignPad and signature in reproducible form including biometric information. The complete signature data record is stored in the database.

Both options are permissible according to the GDPR. GDPR does not require a written form in the sense of Section 126 German Civil Code (BGB) according to which a handwritten signature would have to be placed below the consent form. Recital 32 GDPR describes some possibilities how consent could be gathered:

> *"(...) This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data."*

According to GDPR an effective consent can already be declared through conclusive acting. Only because of the principle of accountability should an electronic or written consent be obtained.

However, it should be noted that the national legislator could also prohibit the processing of special categories of personal data on the basis of consent (Article 9 Section 2a) GDPR). This means that the member states can also stipulate further requirements. A member state could, for example, allow only written form or an electronic form. If the legislator can completely exclude the instrument of consent, then it can a fortiori allow consent under increased requirements. This applies in particular to genetic data, biometric data and data concerning health, as for these special sub-categories Article 9 Section 4 GDPR provides a specific opening clause:

> *"Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."*

The German legislator did not transpose this into the BDSG. Only in the area-specific data protection law there are occasionally special requirements.

While § 67b para. 2 Tenth Book of the Social Code (SGB X) so far only contains a provision according to which consent to the processing of personal data "should" be given in writing or electronically for verification purposes in accordance with Art. 7 GDPR, although this is not a valid condition for consent, it is now proposed to regulate in a new sentence 2 that consent to the processing of genetic, biometric or health data (or company and trade secrets) must be given in written form or electronically, unless another form is appropriate due to special circumstances. It follows from the explanatory memorandum of the bill that this would no longer be only a requirement of admissibility but also a requirement of effectiveness: With reference to the opening clause of Art. 9 para. 4 GDPR, a stricter formal requirement would only be necessary for the aforementioned categories of data, in order to maintain the level of protection of the old provision of Section 67b para. 2 sentence 2 SGB X[old version] to the permissible extent. At the same time, the draft law provides that Section 67b para. 3 SGB X is to stipulate for processing for research purposes that a special circumstance under which a deviation from the aforementioned formal requirement is possible exists if the research purpose would be significantly impaired by obtaining written or electronic consent. In this case the reasons should be recorded. What "in writing" according to the SGB X would

mean is not explicitly defined. It is to be assumed, however, that this refers to the requirements of Section 126 BGB.

The requirement of written consent also arises from the AMG, the MPG, the StrlSchV. With regard to the old regulations still applicable here, however, changes are to be expected due to current draft laws.

For logistical reasons, the original paper consent remains at the respective location and only a scan of the document is transmitted in encrypted form to the TTP consent management system.

Is this procedure also legally secure from the point of view of the GDPR?

Article 7 Section 1 GDPR states:

"Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

In the sense of the principle of accountability (Article 5 Section 2 GDPR) a scan will be sufficient in order to demonstrate that the data subject has consented. In a case as described before it would—from our point of view—already be sufficient if there would be a protocol about the ticking of a box. The more it will be sufficient to have a copy of an original consent form. It would however be advisable to choose a scan-option that does not make use of pattern matching.

As a side note: If the consent form includes personal data, especially data concerning health, the transfer of this data should also be covered by the consent.

How is the use of signature devices, e.g. from sign-o-tec (store biometric data, not only the optical course of the signature) to be seen in relation to the two variants permitted under the German Civil Code (written form requirement or qualified electronic signature)? Under which conditions can Signpads be used hospital-wide for digital collection of the signature and the treatment contract?

German law does not only allow written form or a qualified electronic signature. It would not be necessary to use special signature devices. Therefore one could also use plug-ins for the capture of signatures on mobile terminals or use voice or video recordings of the consenting person.

A major advantage would certainly be that the biometric data could be used to establish a verifiable assignment to the person giving consent. However, such a collection and storage of "biometric data for the purpose of uniquely identifying a natural person" itself is prohibited by Article 9 Section 1 GDPR. The informed consent would also have to cover the processing of biometric data for this reason.

Furthermore, the use of qualified electronic signatures is likely to be ineffective already for practical reasons. According to § 126a para. 1 BGB a signature can be replaced by a qualified electronic signature. However, there will regularly be a lack of the necessary technical prerequisites resulting from the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). Article 3 No. 12 eIDAS Regulation defines a "qualified electronic signature" as an

> *"advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures".*

Only very few patients, hospitals or study sites will be able to provide corresponding signature generation devices and qualified electronical certificates.

> *When is a consent valid: a) only with signature of the participant or b) only with signature of the participant and signature of the informing person?*

Data protection law does not require any other person than the data subject to give a declaration of consent.

> *Are dates on the consent mandatory?*

The indication of a date is not required by law. However, it is recommendable in terms of the principle of accountability.

> *Is an invalid consent merely a quality defect or must it be a mandatory prerequisite for data collection?*

An invalid consent cannot lead to a lawful processing of personal data based on that consent. However not every mistake leads to an invalid consent. In these cases an individual examination is required.

> *What differences must be taken into account in this regard for AMG or MPG studies compared to "normal" studies within the framework of the professional code of conduct?*

Consent serves different purposes even if the reason for obtaining it usually lies in the protection of the general personality rights. Whenever consent is obtained, it must be informed consent. However, the requirements for the type and scope of information may vary. In all cases there is a risk that incorrect consent will be completely ineffective and that actions that nevertheless take place will be unlawful. However, not every mistake leads to an invalid consent. In these cases an individual examination is required. In general, however, the following can be said:

Medical professional law requires consent with regard to treatment. More specifically, it is a permission for a doctor to intervene in the physical integrity of a patient. Requirements for consent to data processing by a physician, on the other hand, do not arise from the professional codes of conduct of physicians. Only the unauthorised disclosure of patient information by a doctor is covered by the medical confidentiality obligation. This may require consent in the sense of a release from the duty of professional secrecy. Formal requirements are not laid down in the professional regulations of doctors. Also **criminal law** Section 203 StGB does not articulate such requirements. Of course, evidence of the existence of consent is recommended, which is why written consent is often obtained. However, with "normal" studies **data protection law** applies as well. For this we can refer to the above.

Other requirements are sometimes stipulated in specific laws. These include the AMG, the MPG and also the Radiation Protection Ordinance (StrlSchV).

Section 40 para. 1 no. 3 lit. b) **AMG** regulates an informative talk and written consent in medical ethical terms and Section 40 para. 1 no. 3 lit. c) AMG regulates information and written consent in data protection terms. The informative talk has to follow the stipulations according to Section 40 para. 2 S. 1 AMG, which states that the person concerned shall be informed of the nature, significance, risks and implications of the clinical trial **by an investigator** or a **member of the trial group who is a physician** or, in the case of a dental trial, a **dentist**, and of his or her right to terminate participation in the clinical trial at any time, and shall be provided with a generally understandable educational document.

Section 40 para. 2a AMG is concerning the data protection information and lists certain aspects that a participant has to be informed about. In this case the law does not say, that the information has to be provided by a certain person.

Section 20 para. 1 S. 4 No. 2 **MPG** in conjunction with Section 20 para. 2 No. 2 MPG states that the person concerned has to give consent in written form after having had an informative talk with a physician, in the case of medical devices intended for dentistry also by a dentist, about the nature, significance and scope of the clinical trial. The MPG does not distinguish between consent to participation in clinical trials and consent to data processing.

Section 133 **StrlSchV** obliges the radiation protection supervisor (Strahlenschutzverantwortlicher) to ensure that consent is obtained and that information is being provided and an informative talk takes place. Consent in this case covers both the processing of personal data and the use of radioactive substances or ionising radiation on the participants body and examinations that are necessary before, during and after the use of radioactive substances or ionising radiation on the participants body in order to control and maintain his/her health (Section 134 para. 1 S. 1 StrlSchV).

Section 135 para. 1 StrlSchV requires that comprehensible written information is handed out in which the nature, significance, scope and risks of the use of the radioactive substances or ionising radiation are explained and the person involved in the research project is informed of the conditions and duration of the use and of the possibility of withdrawing consent in accordance with Section 134 para. 1 s. 1.

Section 135 para. 2 StrlSchV contains the requirement for an informative talk. The study participant must be informed and questioned by the physician or dentist in charge of the application of radioactive substances or ionising radiation by a doctor or dentist appointed by him whether radioactive substances or ionising radiation have already been applied to him. In the case of applications requiring approval, the physician or dentist in charge must have the necessary expertise in radiation protection. The information shall include the aspects referred to in paragraph 1. The radiation protection supervisor shall ensure that records are kept of the information and questioning.

Are there different validity criteria for consents for the collection and publication/ transfer of data?

Before the GDPR came into force, a distinction was made in the (old) BDSG between collection, processing and use of personal data. After the model of the GDPR this differentiation was largely given up in the German data protection law. A consent, that refers to the processing of personal data, covers therefore all conceivable processing. Special requirements can result for the transmission in countries outside the EU (see article 49 Abs. 1 lit. a) GDPR). Whenever data is transmitted, it must of course be assessed whether this could violate professional secrecy.

In contrast to consent to participate in a study and the related data processing described above, the information about the publication must be explicitly related to this publication. Most laws contain specific provisions for the publications of personal data in the context of scientific research, e.g. Section 27 para. 4 BDSG, Section 13 para. 4 LDSG-SH, Section 37 para. 4 s. 3 LKHG-MV, Section 25 para. 4 BlnLKG. For the study participant it should be pointed out in particular the fact that data can possibly not be taken back after it has been published and an erasure claim may be limited to the right to be forgotten according to article 17 Abs. 2 GDPR.

5.2 Consents (before 25/05/2018)

The TTP administers consents of patients who were collected before 25.05.2018. Individual consents use a passage on the use and transfer of data (including "third countries with lower data protection levels"). A large number of patients have agreed to this passage.

Are these still permissible under Chapter 5 of the GDPR or must new consent be obtained?

How does this regulation behave in particular with regard to cooperations with the USA?

5.2.1 General Information on the Continuation of Declarations of Consent

Consents that were effectively given under the former legal situation generally remain valid. This is the case if a minimum standard has been met so that a core information content existed at the time of consent. Recital 171 GDPR states explicitly:

"Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation."

In recital 42 GDPR it is described as core information content of consents that a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms and informs the person concerned at least about who the responsible person is and for which purposes his personal data should be processed. It can therefore be assumed that consent was only given voluntarily if the data subject has been given a genuine or free choice or is able to refuse or withdraw consent without detriment.

However, the fact that the general information obligations and thus the contents of a data protection declaration are changed by the GDPR does not affect the validity of the consent itself. This view is also shared by supervisory authorities.[10]

5.2.2 Third Country Transfer

A third country transfer is a data transfer to a country that does not belong to the European Union or the EEA states. Third Country Transfers are addressed in Chapter V of the GDPR (Article 44 GDPR et seq.).

With regard to the transfer of data to third countries for which no adequacy decision has been taken, the following applies:

In the case of a transfer of a third country, a 2-step-test of legality shall be carried out. In **a first step**, the data controller must ensure that the transfer meets

10 *Bayerisches Landesamt für Datenschutzaufsicht*, Kurzpapier IX—Einwilligung nach der DS-GVO; https://www.lda.bayern.de/media/baylda_ds-gvo_9_consent.pdf.

the general conditions for the processing of personal data. All general requirements of the GDPR are to be met as if it was a processing without reference to third countries. It should be noted though, that a third country transfer may lead to further duties. For example the data subject shall be informed according to Article 13 para. 1f) GDPR about

> *"(...) the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49 (1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."*

In the case of third country transfers, as a **second step** follows in which it is examined whether an adequate level of data protection in relation to the legal framework of the European Union has been achieved in a recipient country or whether suitable or appropriate guarantees have been implemented (Article 45–47 GDPR) or whether one of the exceptions in Art. 49 GDPR is applicable.

Adequacy Decision (Article 45 GDPR)

According to Article 45 GDPR a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer does not require a transfer specific authorisation. Only the general requirements of the GDPR have to be met.

At present, a general adequacy decision exists only for the following countries:

- Andorra
- Argentina
- Australia
- Canada (restricted)
- Faroer Islands
- Guernsey
- Isle of Man
- Israel (restricted)
- Japan[11]
- Jersey
- New Zealand
- Switzerland
- Uruguay

11 http://europa.eu/rapid/press-release_IP-19-421_en.htm

There is a special constellation with regard to the **United States of America**: *Although there is no general adequacy decision concerning the US*, American companies have the option of self-certification under the so-called **EU-US Privacy Shield**[12]. *In this case the Commission treats the self-certified companies as if they were in a country with an adequacy decision.*

No Adequacy Decision

In a case where there exists no adequacy decision of the Commission, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (Article 46, 47 GDPR) unless one of the derogations for specific situations according to Article 49 GDPR applies.

Appropriate Safeguards

Article 46 para. 2 GDPR states that **without requiring any specific authorisation** from a supervisory authority the following safeguards may be used:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47 GDPR;
- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93 (2) GDPR;
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93 (2) GDPR;
- an approved code of conduct pursuant to Article 40 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism pursuant to Article 42 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Also, however **subject to authorisation from the competent supervisory** authority, safeguards may be:

- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

12 https://www.privacyshield.gov/welcome.

- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Derogations for specific situations

If the cases mentioned so far are not suitable, the exceptions under Article 49 can also be used. According to Article 49 para. 1 s. 1 GDPR at least one of the following conditions must be met:

- **explicit consent** to the proposed transfer, after having been **informed of the possible risks** of such transfers for the data subject **due to the absence of an adequacy decision and appropriate safeguards**;
- transfer is **necessary for the performance of a contract** between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- transfer is necessary for **important reasons of public interest**;
- transfer is necessary for the **establishment, exercise or defence of legal claims**;
- transfer is necessary in order to **protect the vital interests of the data subject** or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made **from a register** which according to Union or Member State law is intended to provide information to the public and which is **open to consultation** either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

According to Article 49 para. 1 s. 2 GDPR transfer shall also be admissible if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14 GDPR, inform the data subject of the transfer and on the compelling legitimate interests pursued.

5.2.3 Conclusion

The question of whether declarations of consent obtained before 25 May 2018 continue to be valid must be answered on a case-by-case basis and by examining the complete declaration of consent. A mere reference to a transfer of data to insecure countries may already be uncertain, even under the former legal situation.

In any case, the necessary information on the data processing operations should be provided in an up-to-date form.

5.3 Consent (after 25/05/2018)

> *Does the GDPR permit the following consent clause? What content adjustment would have to be made if necessary?*
>
> *"Pseudonymised data and biomaterials may be transferred to countries for which the European Commission has not determined an adequate level of data protection".*

The above applies accordingly, however, in the case of new declarations of consent to be obtained, the requirements of the GDPR (in particular Article 6, 7, 9 GDPR) must be complied with. The proposed sentence should only be included in a declaration of consent if consent is required for the legitimation of a data transfer to a third country (Article 49 para. 1 s. 1a) GDPR). Otherwise, it is sufficient to provide information within the framework of the data protection declaration, which is made in accordance with Article 13, 14 GDPR.

As far as "biomaterials" are concerned, the data subject does not have to be informed about the transfer to a third country. Biomaterials are not considered personal data under to the GDPR. Even if personal information, in particular genetic data or data concerning health, could be extracted from biomaterials, the biomaterial itself is not considered personal data. Article 4 No. 13 GDPR defines genetic data as

> *"(...) personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."*

The wording therefore requires an **analysis of a biological sample** in which data are obtained (see also recital 34).

5.4 Dealing with different consent versions

As part of the study preparations, the declaration of consent for a new study is given to an ethics committee. This committee prepares an ethics vote for the submitted documents in the current version. The TTP assumes that in a study with a valid ethics vote, study participants may only consent to the respective declaration of consent. If the content of a consent changes, it must be voted on again and a new version of the consent must be created accordingly.

If a multicentre study decides to change the content of a consent form, it must in most cases be submitted to all competent local ethics committees. It makes operational sense that uniform versions are always used across all centres. In the case of a version change, the trustee assumes that recruitment must continue with the consent form voted on (e.g. 1.0). Even if the study centre (e.g. Berlin) already has a vote for a newer version (e.g. 1.5), all centres must (according to the previous definition) recruit with the existing and universally voted version (e.g. 1.0) until all centres have a uniformly voted version. What is your legal assessment of this situation? Are study centres allowed to recruit a study with different consent versions at all, or do they have to be uniform throughout the study?

A new ethics vote will only normally be necessary if significant changes have been made. If it makes a difference whether the old version or the new version of the informed consent is used, it should be noted that either all study participants receive and sign the new version of the informed consent, or the research project must be conducted heterogeneously according to the different consents.

There is no universal rule that applies to all areas of scientific research according to which a single ethics vote by a central ethics committee is sufficient. However, there are exceptions for some areas of medical research:

In the field of **clinical trials of medicinal products**, multi-centre studies benefit from simplifications provided for in EU law which have been implemented in national law. In the case of multicentre clinical trials of medicinal products, Article 7 Directive 2001/20/EC provides as follows:

"For multi-centre clinical trials limited to the territory of a single Member State, Member States shall establish a procedure providing, notwithstanding the number of Ethics Committees, for the adoption of a single opinion for that Member State.

In the case of multi-centre clinical trials carried out in more than one Member State simultaneously, a single opinion shall be given for each Member State concerned by the clinical trial."

The first subparagraph of Article 7 Directive 2001/20/EC was implemented in Section 40 para. 1 S. 2 AMG. It states that the ethics committee responsible at

the site of the principal investigator acts as the lead ethics committee and that its vote alone is decisive. According to the second subparagraph of Article 7 Directive 2001/20/EC in an international multi-center study, however, one ethics vote per country is required. It should be noted that **in the future under the 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 (so-called clinical trials regulation—CTR) there will no longer be a comparable provision to Article 7 Directive 2001/20/EC. The regulation of responsibilities will, however, be left to the Member States (see Recital 18 of the CTR).

EU law on **medical devices** does not regulate the competence of ethics committees in multi-centre studies. This applies both to the old EU law with Directives 93/42/EEA, 90/385/EEA and 98/79/EC as well as the new Regulations 2017/745 and 2017/746. Provisions, however, result from Member State law, which provide rules similar to the ones of AMG: Section 22 para. 1 S. 2 MPG stipulates that in the case of a trial conducted by several investigators, the application must be submitted to the independent ethics committee responsible for the principal investigator or head of the clinical trial. Section 22 para. 1 S. 3 MPG expressly states that an ethics vote is sufficient for multicentre studies. According to Section 5 para. 2 S. 2 Ordinance on Clinical Trials of Medical Devices (MPKPV), multi-centre clinical trials or performance evaluation trials conducted by more than one trial site within the scope of the MPG shall be evaluated by the competent ethics committee, with the other ethics committees involved being consulted. Pursuant to Section 5 para. 2 sentence 3 MPKPV, the other ethics committees involved only examine the qualification of the reviewers and the suitability of the review sites in their area of responsibility. The comments made in this regard shall be taken into account. Further information must be documented, but need not be considered by the competent ethics commission (Section 5 para. 2 p. 5 MPKPV).

Furthermore, Section 36 para. 2 S. of the **Radiation Protection Act** (StrlSchG) stipulates that only one ethics vote is required for multi-centre studies. There is no regulation as to which ethics commission would be in charge. The European legal basis of the "Council Directive 2013/59/EURATOM of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom" contains no provisions on the competence of ethic committees for international multicentre studies beyond the necessity of an ethics committee decision regulated in Art. 55 para. 2 lit. e). However, it can be assumed that this can be determined following the example of the AMG or MPG.

5.5 Withdrawal of a Declaration of Consent/Study Exclusions

Within the scope of the withdrawal process, the data of a participant will be anonymised. The medical data is also locked for further data transfer and can normally not be processed further.

How should this regulation be viewed in connection with AMG/MPG studies? Can data still be supplemented or edited after the withdrawal?

The interaction of GDPR, BDSG and AMG or MPG is complex. The directly applicable GDPR constitutes the basic part of EU data protection law. On the basis of the opening clauses contained in the GDPR, the Member States may in some cases adopt their own data protection regulations. In the case of the processing of health data which is relevant here, the GDPR provides that processing may be carried out either on the basis of a consent pursuant to Article 9 para. 2 lit. a) GDPR, provided that this is not excluded by Member State law, or on the basis of a legal basis of authorisation in Member State law.[13] The opening clauses in Article 9 para. 2 lit. h) GDPR (individual health care), Article 9 para. 2 lit. i) GDPR (public health) and Article 9 para. 2 lit. j) GDPR (scientific research) can be considered for the latter.

The German legislator has provided general regulations on the processing of health data in Section 22 BDSG and Section 27 BDSG for purposes of health care and research. The relationship of the BDSG to other federal laws such as the AMG or the MPG is governed by Section 1 para. 2 sentence 1, 2 BDSG:

"Other federal data protection legislation shall take precedence over the provisions of this Act. If such legislation does not govern a matter conclusively or at all which is covered by this Act, then this Act shall apply."

Specific Sections of AMG and MPG may be considered as other federal data protection legislation in that sense.

For this reason, the data protection related provisions of the AMG and the MPG take precedence over the provisions of the BDSG.

5.5.1 Medicinal Products Act (Arzneimittelgesetz—AMG)

The data protection requirements for the conduct of a clinical trial of a drug in humans are currently regulated in Section 40 para. 1 sentence 3 no. 3c, para. 2a AMG. These national regulations are based in part on provisions of Directive 2001/20/EC on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good

13 The directly applicable legal bases of Art. 9 para. 2 GDPR are not relevant in the constellations relevant here.

clinical practice in the conduct of clinical trials on medicinal products for human use.

In future, the requirements for clinical trials with medicinal products for human use will be regulated by a directly applicable regulation, namely Regulation 536/2014/EU on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. Only supplementary regulations are then to be found in Sections 40 etc. AMG-new.

Pursuant to Article 99 of Regulation 536/2014/EU, the Regulation only applies six months after the publication of the notice on the Functioning of the EU Portal and the EU Database referred to in Article 82 para. 3 of Regulation 536/2014/EU in the Official Journal of the European Union. Such notification has not yet been published.

According to Section 40 para. 1 sentence 3 no. 3c AMG, the data protection consent required for conducting a clinical trial—in contrast to the non-data protection consent according to Section 40 para. 1 sentence 3 no. 3b, para. 2 AMG—is indispensable. The inadmissibility of the withdrawal of the data protection consent results from the corresponding information provision of Section 40 para. 2a sentence 1 no. 2 AMG, according to which it must be clarified that the consent according to Section 40 para. 1 sentence 3 no. 3c AMG cannot be withdrawn. This provision, which is primarily concerned with information, also constitutes the inadmissibility of the withdrawal of the declaration of consent.

The aim is to prevent a participant from jeopardising the reliability of the study by subsequently preventing the processing of his data by withdrawing his consent.[14]

The provision of Section 40 para. 1 sentence 3 no. 3c AMG conflicts with Article 7 para. 3 sentence 1 GRPR as well as with Article 13 para. 2 lit. c), Article 14 para. 2 lit. d) and Article 17 para. 3 lit. b) GDPR. In particular Art. 7 para. 3 sentence 1 GDPR determines that the person concerned has the right to withdraw its consent at any time. The legality of any data processing carried out up to that point shall not be affected by such withdrawal.

However, Section 40 para. 2a sentence 1 no. 2 AMG can be justified on the basis of an opening clause in favour of the Member States. The GDPR expressly does not contain an opening clause relating to consent which allows a non-withdrawable form. However, it should be noted that the processing of personal health data is not only possible under Art. 9 para. 2 lit. a) GDPR on the basis of consent, but also without consent in accordance with legal authorisation (cf. Art. 9 para. 2 lit. b) to j) GDPR). The processing of such data after a withdrawal of consent does not therefore necessarily have to be regarded as data processing on the basis of a continuing (non-withdrawable) consent, but could

14 *Rehmann*, AMG, 4. Aufl., 2014, § 40 Rn. 13.

rather be interpreted as data processing without (continuing) consent on the basis of a statutory order. The designation as "non-withdrawable consent" would then only be a legally abridged wording to the effect that certain data processing operations are nevertheless permissible after the withdrawal of consent. The idea of allowing data processing to be carried out on the basis of a statutory regulation becomes clear in the future version of Section 40b para. 6 sentence 3 no. 2 AMG-new. Accordingly, "in the event of withdrawal" of consent, "the stored data may continue to be used" under the conditions specified in the provision.

For the creation of such a legal basis in national law, the Federal legislator can rely on the opening clause of Article 9 para. 2 lit. i) GDPR. The clause enables the Member States to create national regulations which allow the processing of health data for reasons of public interest in the field of public health. In particular, the clause mentions the guarantee of high quality and safety standards for medicinal products as such a public interest. Regulations which permit the processing of health data in the context of a clinical trial even after the withdrawal of consent guarantee the reliability of data from clinical trials (cf. recital 76 of Regulation 536/2014/EU) and serve to reliably determine the effects of the medicinal product to be tested. In the case of lawful data processing using Art. 9 para. 2 lit. i) GDPR, the right of the data subject to have his personal data deleted is also excluded (Art. 17 para. 3 lit. c) GDPR).

In fact on 5th September 2018, the Federal Government passed a draft law on the 2nd Act to Adapt Data Protection Law to Regulation (EU) ("Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU—2. DSAnpUG-EU"). With this in particular area-specific data protection regulations are to be adapted to the provisions of the GDPR. Article 18 of the draft also provides for an amendment according to which consent is to be withdrawable under the AMG, but further processing may still remain permissible. The logic represented above would be corresponded with this regulation.

5.5.2 Medical Device Act (Medizinproduktegesetz—MPG)

The possibility to withdraw consent implemented under Section 20 Para. 2 sentence 2 MPG is in line with the compelling regulations of the Art. 7 Para. 3 sentence 1 GDPR as well as the Art. 13 para. 2 lit. c), Art. 14 para. 2 lit. d) and Art. 17 para. 3 lit. b) GDPR. In particular Art. 7 para. 3 sentence 1 GDPR determines that the person concerned has the right to withdraw its consent at any time. A provision stating that personal data already collected may be further processed even after withdrawal does not yet exist. Any further processing of the data would therefore be unlawful. The data must be deleted.[15]

15 Spickhoff/Listl-Nörr, 3. Aufl. 2018, MPG § 20 Rn. 9.

However, Article 83 No. 2 lit. bb) of the 2. DS-AnpUG-EU (Draft law) stipulates that such a right of further processing is to be implemented in Section 20 para. 2 S. 3 MPG-new in the future. According to the draft law, stored data could be to be processed as far as this is necessary to achieve the objectives of the clinical trial or not to seriously impair them or to ensure that the legitimate interests of the data subject are not impaired.

Under the Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (so-called Medical Device Regulation—MDR), the revocability of consent is governed directly by EU law. Article 62 para. 5 MDR reads as follows:

> *"Any subject, or, where the subject is not able to give informed consent, his or her legally designated representative, may, without any resulting detriment and without having to provide any justification, withdraw from the clinical investigation at any time by revoking his or her informed consent. Without prejudice to Directive 95/46/EC, the withdrawal of the informed consent shall not affect the activities already carried out and the use of data obtained based on informed consent before its withdrawal."*

The same applies under the "Regulation (EU) 2017/746 of the European Parliament and of the Coucil of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU to clinical trials of in vitro diagnostic medical devices" *(so-called IVDR) according to* Article 58 para. 6 IVDR.

6 Legal consequences of withdrawal

Paper-based consents include the source-specific primary pseudonym of the participant. Should this pseudonym be blacked out/cut out in the consent?

Withdrawal of a patient means the blocking and anonymisation of the data. The data will only be deleted upon explicit request. Is this procedure permissible?

As a rule, data must already be **erased** when the consent is withdrawn. However, there are exceptions to this rule.

Art. 17 para. 1 GDPR states that the controller shall have the obligation to erase personal data without undue delay where the data subject withdraws consent on which the processing is based according to point (a) of Article 6 para. 1, or point (a) of Article 9 para. 2, and where there is no other legal ground for the processing. In cases where there is no other legal basis on which further processing is lawfully possible, personal data must therefore be erased without the explicit request of the data subject.

The question of whether a different legal basis exists must be answered depending on the type of study. As already mentioned, for example the AMG provides such legal grounds.

However, according to the view expressed here, anonymisation, in which all copies of the data records are also anonymised, amounts to erasure. With the erasure of the data the data protection law is no longer applicable. The same

effect can be achieved by anonymisation. From a legal point of view, the question can be raised whether anonymisation is sufficient to fulfil the erasure obligation. Anonymisation would have the great advantage for the person responsible that the (no longer personal) individual data remaining after successful anonymisation could be reused, for example for the purpose of statistical evaluations. They may therefore continue to be of considerable value, which would be lost if they were completely erased. At the same time, however, the applicability of the right to informational self-determination ends with the loss of personal reference.

Already according to the old legal situation it was therefore well recognised that also the anonymisation of data can represent a form of deletion.[16] This does not result directly from the wording of the law, but sense and purpose of the regulation speak for it, since an anonymisation represents the complete abolition of the personal reference.[17] The prevailing opinion was based on the assumption that according to Section 35 BDSG (old version) the person concerned could demand anonymisation or pseudonymisation instead of deletion.[18] The GDPR contains no legal definition of the erasure. As a subcategory of the term "processing", the GDPR lists the two terms "erasure" and "destruction" in Article 4 No. 4 GDPR. From this differentiation, it can be derived that erasure does not presuppose a destruction compellingly.[19] However, there are no indications that a definition deviating from the previous understanding might emerge. With regard to the means and procedures of deletion, the person responsible is entitled to choose how to erase data.[20]

In December 2018, the Austrian data protection authority issued a decision in which it stated that a deletion claim can be met by anonymisation.[21] For the assumption that anonymisation is equivalent to erasure, a database must be generated that no longer contains any personal data.[22] It is not sufficient to merely change the data organisation in such a way that "targeted access" to the data concerned is excluded.[23] This would mean that it would not be sufficient to delete an identifier for a data set, an otherwise leave the data set unchanged (virtually anonymous data). Even if a targeted access for a data record would no longer be possible without the identifier, e.g. with the help of a search function, this would not be equivalent to erasure by anonymisation.

16 BeckOK DatenSR/*Brink*, 20. Ed. 1.2.2017, BDSG § 35 Rn. 26, beck-online; *Dix*, in: Simitis, BDSG, 8. Aufl., 2014, § 35 Rn. 45; *Plath/Schreiber*, in: Plath, BDSG/DSGVO, 2. Aufl., 2016, § 3 BDSG Rn. 52.

17 *Dix*, in: Simitis, BDSG, 8. Aufl., 2014, § 35 Rn. 45.

18 *Meents/Hinzpeter*, in: Taeger/Gabel, BDSG, 2. Aufl., 2013, § 35 Rn. 17; *Dix*, in: Simitis, BDSG, 8. Aufl., 2014, § 35 Rn. 45.

19 *Kamann/Braun*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 17 Rn. 32 (m.w.N); OLG Frankfurt, Urteil vom 06. September 2018—16 U 193/17—, Rn. 51, juris.

20 *Kamann/Braun*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 17 Rn. 36.

21 ECLI:AT:DSB:2018:DSB.D123.270.0009.DSB.2018.

22 BeckOK DatenSR/*Schild* BDSG, 20. Ed. 1.5.2017, § 3 Rn. 98, beck-online.

23 ECLI:AT:DSB:2018:DSB.D123.270.0009.DSB.2018.

Therefore it would all the more be insufficient to only store IDAT in a separate file.[24] With reference to WP 216 of the Article 29 Data Protection Working Party, the Austrian supervisory authority states, that only if the controller aggregates the data on one level so that no individual events can be identified can the resulting database be described as anonymous.[25] Log files may also no longer contain any data that could enable the identification of the data subject.[26]

Art. 17 Abs. 2 GDPR contains the hint in the context of the "right on being forgotten" that all "copies or replications" are covered by a deletion request. Therefore, it remains the case that all copies must be deleted or made anonymous. This also follows directly from the considerations on the effectiveness of anonymisation.[27] German legislation does not provide for a different consideration.

> *When implementing a withdrawal, biomaterials must be destroyed and proof of destruction (technical notification, completed paper form, scan) must be provided.*
>
> *Is a simple database entry in the Audit Trail sufficient or do we have to have an original paper for legal reasons and keep it in a written form according to the German Civil Code (BGB)?*
>
> *What exactly is TTP responsible for? Control of destruction or only request for destruction and obtaining confirmation of success?*

The law of biobanks has not been codified uniformly in Germany.[28] Legislative proposals have not been implemented in the past. Therefore, the various legal issues are subject to different framework conditions resulting from the legal sub-areas concerned in an individual case.[29]

First of all, the handling of biomaterial per se does not constitute the processing of health data.[30] Only the information generated after an examination of the biomaterials or information linked to the biomaterial can be person-related. Also in these cases it is crucial that it is not just anonymous data about a person, but that the person is identifiable. Data protection claims for deletion could be satisfied by anonymising the data without necessarily destroying the biomaterial.

The legal requirements for handling human biomaterials must also be considered separately from data protection law. The question of the necessity of de-

24 *Greve*, in: Auerhammer, DSGVO/BDSG, 5. Aufl., 2017, § 40 BDSG Rn. 14.
25 ECLI:AT:DSB:2018:DSB.D123.270.0009.DSB.2018.
26 ECLI:AT:DSB:2018:DSB.D123.270.0009.DSB.2018.
27 See also *Klabunde*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 4 Rn. 16.
28 There are only a few legally binding regulations which expressly regulate the handling of biosamples, e.g. § 12 HmbKHG.
29 Albers, MedR2013, 483.
30 See Part II.5.3

stroying biomaterials after the revocation of consent to the use of biomaterials arises essentially from civil law and constitutional requirements.[31] While the living human body cannot be property in the sense of § 90 BGB, this changes if a body part or tissue is removed from the body at least if is not to be re-implanted into the body.[32] Once biomaterial has been removed from a body, it will be the property of the patient. The patient can then transfer the ownership of the biomaterial to another party such as a biobank.

However, since biomaterial contains DNA and thus, according to prevailing opinions, is subject to the protection of human dignity pursuant to Article 1 para. 1 GG, the ownership of biomaterial is superimposed by the general right of personality.[33] As a consequence, the prevailing opinion in legal literature requires consent to the use of biomaterial. It is the nature of consent to be revocable.[34] Consequently, if consent to the use of the biomaterial is withdrawn, it must not be used contrary to the will of the person concerned in a way that infringes his or her personal rights. As a rule, the destruction of the biomaterial may therefore be appropriate.

However, there are **no explicit rules requiring specific proof of destruction**. Such an obligation does not follow from an analogous application of data protection regulations. Because also the GDPR does not require any proof about the erasure of data. The information that data about a person have been erased would require that again data about this person would have to be stored. This would counteract the purpose of the erasure claim. On the other hand, an entry in the Audit Trail that biomaterial with a specific registration number has been destroyed should be admissible and sufficient. There should be a concept for dealing with deletions and destruction.

Responsibility for the destruction of biomaterial usually lies with the biobank, but not with TTP. As a rule, the TTP will not have access to the biosamples and will therefore not be able to carry out the destruction. The obligations of the TTP will be determined on the basis of the respective cooperation agreements. As a rule, it will be sufficient to forward corresponding erasure requests or destruction requests.

This would correspond with the right to be forgotten according to Art. 17 para. 2 GDPR, which also provides for an obligation to inform the data recipients about an erasure request, but does not prescribe that a confirmation of the erasure must be obtained.

31 Albers, MedR2013, 483 (485ff.)

32 BGH NJW 1994, 127 (128); *Pommerening/Drepper/Helbing/Ganslandt*, Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, Generische Lösungen der TMF 2.0, 2014, S. 51; Albers, MedR2013, 483 (486); With a view that even if there is an intention of reimplantation, ownership already arises: MüKoBGB/Stresemann, 8. Aufl. 2018, BGB § 90 Rn. 27.

33 BGH NJW 1994, 127 (128), Albers, MedR2013, 483 (486).

34 Spranger, NJW 2005, 1084 (1087).

7 Standard Operating Procedure (SOP)

According to Art. 6–11 GDPR, all data processing operations should be able to be agreed to separately. In addition, the data processor must comply with an accountability obligation (which data have been agreed to) and a process for the withdrawal procedures must be implemented. Within the framework of the Trusted Third Party, the consent management gICS and Standard Operating Procedures are used for these purposes. Are the requirements of the GDPR sufficiently implemented in this way?

GDPR does not require that consent has to be given separately concerning every single data processing operation or step. However, it is recommended that, in cases where consent is required, consent should be modular in structure to the extent that delimitable purposes and processes that are not necessarily connected can be addressed independently of one another.[35] Standard Operating Procedures can be suitable to achieve this if they are designed to address specific processing and document consent. They can be helpful in a way that omission are avoided and documentation gets automated in the process.

The gICS[36] consent management system from our perspective would be suitable.

35 *Schaar*, ZD 2017, 213, Anpassung von Einwilligungserklärungen für wissenschaftliche Forschungsprojekte, S. 215

36 Bialke et al. MAGIC: once upon a time in consent management—a FHIR® *tale*; J Transl Med (2018) 16:256 https://doi.org/10.1186/s12967-018-1631-3

8 Ethics Committee Vote

Is the existence of an ethics vote a mandatory prerequisite for the activation of a site and the start of data collection at this site?

Whether an ethics vote is required or not depends on the nature of the research project and the persons involved. The GDPR does not demand an ethics vote for the admissibility of a data processing for the purpose of the scientific research. The entire GDPR takes only in recital 33 reference to the adherence to ethical standards for the special case of a Broad Consent. Nevertheless, the requirement for an ethics vote may follow from specific EU law or German law depending on the type of study and the persons involved (cf. tab. 1).

It should be noted, that whenever the research project is carried out by **physicians**, the regulations of medical professional law must be followed. In a Model Professional Code Of Conduct (MBO-Ä) which is not legally binding, the German Medical Association (Bundesärztekammer) has formulated guidelines which have been converted into a legally binding professional code of conduct for doctors by the respective medical associations in all seventeen German chamber districts.

Tab. 1 Requirements for an ethics vote depend on the type of study and the applicable law

Type of Study	EU law	German law
Clinical trial (medicinal products)	■ Article 3 para. 2 lit. a) Directive 2001/20/EC ■ Article 3 lit. a), Article 4 subparagraph 1 and 2 Regulation 536/2014/EU	■ Section 40 paragraph 1 sentence 2 AMG
Clinical trial (medical devices)	■ Article 15 Directive 93/42/EC ■ Article 10 Directive 90/385/EC ■ Article 62 para. 3 lit. b) Regulation (EU) 2017/745 ■ Article 58 para. 5 lit. b) Regulation (EU) 2017/746	■ Section 20, paragraph 1, sentence 1, var. 1 in conjunction with Section 22 MPG
Application of radioactive substances or ionising radiation to humans for the purpose of medical research	■ Article 28 lit. a) in conjunction with Article 55 para. 2 lit. e) Council Directive 2013/59/EURATOM	■ Section 31, paragraph 4, no. 5 in conjunction with Section 36 Radiation Protection Act (StrlSchG)

Section 15 para. 1 of the MBO-Ä reads as follows:

> *"Physicians who participate in a research project which invades the mental or physical integrity of a human being, or uses human body material or data which can be traced to a particular individual, must ensure that advice on questions of professional ethics and professional conduct associated with the project is obtained from an Ethics Committee established at the responsible Chamber of Physicians, or from another independent, interdisciplinary Ethics Committee set up according to state law, before conducting the research. The same applies prior to conducting legally permitted research on viable human gametes and living embryonic tissue."*

The Professional Codes Of Conduct for physicians in Mecklenburg-Western Pomerania and Berlin, for example, stipulate the same or comparable requirement for an ethics vote.

> *In what form and to what extent can or must the data processor (TTP) prove the existence of the ethics vote and possibly other legal bases as a prerequisite? Who bears which responsibility?*

The responsibility for obtaining the necessary documents, such as consents, approvals and ethical votes, lies with the person responsible for the research project, in the case of clinical trials the sponsor, but not the TTP. Should TTP nevertheless wish to insure that all documents are available, a simple copy or scan would suffice for this proof, provided that there are no reasonable doubts as to their authenticity.

What is the legal (not: contractual) minimum standard before the data processor can perform his services in conformity with the law, what requirements must be met before the TTP "activates" a study centre, a study or a project?

Independent data trust agencies, such as the TTP, are not regulated by special laws when it comes to ethical votes. Trust agencies should conclude necessary contracts, for example, contracts on data processing according to Art. 28 GDPR, if this is necessary in an individual case. Depending on the tasks of the TTP and its legal independence an agreement according to Article 26 or Article 28 GDPR may have to be in effect before personal data is being processed.

In EU projects: To what extent is the TTP obliged to check the correctness of the ethics vote in the national language (e.g. Greek), or is work on a "basis of trust" sufficient?

As TTP is not responsible for the accuracy, authenticity and efficacy of any ethics vote or approval, no review is required by law. However, a check and, if necessary, a verified translation is recommended in order to limit a possible liability.

9 Quality assurance in the Trusted Third Party

The declaration of consent is considered a central legal document in order to legitimise the processing of study participant data. Therefore, quality assurance measures are carried out on these documents and data in the TTP. As mentioned above, the TTP sends monthly quality reports with specific deficiencies on declarations of consent that require revision. These can be misspelled names, missing signatures or insufficiently marked consents.

The Trusted Third Party of the DZHK currently exclusively supervises multicentre studies (more than 120 affiliated centres). The reports are generated on the basis of the study and the centre and are currently transmitted via encrypted communication to a contact person of the student assistant and must be distributed from there.

Is the above procedure sufficient to ensure a centrally controlled verification of the consent status for the release of data and samples? What further measures might need to be taken?

The procedure described is considered admissible. The GDPR does not provide any explicit stipulations for the consent management. However, it is crucial for the execution of the research project that errors are avoided and data integrity is ensured. The processing of the personal data in the sense of an examination, return transmission, correction and renewed examination as well as further processing is therefore a procedure necessary for reaching the pur-

pose of the research project. This must be considered as covered by the declaration of consent.

Encrypted transmission of declarations of consent is required, since the declarations of consent themselves may already qualify as health data. In addition to transport encryption, the data itself should be encrypted so that it cannot be read in the event of intermediate storage by a telecommunications service provider. Keys for decryption should be transmitted via an alternative means of communication.

10 Authorisation of Study Leaders

To date, the central study leaders have had the right to access and at least view all medical, laboratory and image data of a study participant in other centres.

Do these persons also have the right to view all identifying data of the study participants?

What about multicentre studies? Do the German Medicines Act (Arzneimittelgesetz—AMG) and the Medical Devices Act (Medizinproduktegesetz—MPG) studies contain any requirements in this respect?

The term "*study leader*" is not a term used in the German Medical Law. For the purpose of further evaluation, it is assumed that by "study leader" the "*principal investigator*" is meant, as defined in Article 2 lit. f) Directive 2001/20/EC[37] which reads as follows:

"'investigator': a doctor or a person following a profession agreed in the Member State for investigations because of the scientific background and the experience in patient care it requires. The investigator is responsible for the conduct of a clinical trial at a trial site. If a trial is conducted by a team of individuals at a trial site, the investigator is the leader responsible for the team and may be called the ***principal investigator****" [highlighting not in original text]*

37 In that sense also: Pommerening/Drepper/Helbing/Ganslandt, Leitfaden zum Datenschutz in medizinischen Forschungsprojekten—Generische Lösungen der TMF 2.0, 2014, p. 229.

This definition corresponds to the content of Section 4 para. 25 AMG, where, however, no separate term is coined for the head of the group. A Definition equivalent to Article 2 lit. f) Directive 2001/20/EC can be found in Section 3 No. 24 MPG.

None of these laws stipulate that a principal investigator may not have access to IDAT or must have such access. Therefore, the general principle is that those individuals who need access to IDAT to perform their duties in a research project should have access to that data. Conversely, persons who do not require IDAT must be excluded. If this is to be defined using generic role concepts, it is recommended to restrict access by default and to grant further authorisations if this is necessary in respect to the specific research project in view of the circumstances of the individual case. For example, if a principle investigator in a multi-center setting has mainly a coordinating function with regard to the different study sites, it would most likely not be necessary that the principal investigator has access to IDAT.

It should be noted that apart from the AMG or the MPG the federal state hospital laws applicable to the hospitals in which the study is being conducted may contain more specific rules—this may have to be checked individually for each hospital depending on the type of the study.

If a principle investigator in a multi-center setting has mainly a coordinating function with regard to multi-center studies, it would most likely not be necessary that the principal investigator has access to IDAT.

Of course, a corresponding declaration of consent of the patient enables the processing of IDAT. The patient shall be informed that the principal investigator belongs to the circle of persons who can process IDAT collected during the multicentre trial.

11 Dealing with deceased study participants

In a few cases, the trustee is informed that study participants have died during or after the study. The TTP assumes that the death of a study participant does not result in any changes and that no additional measures need to be taken. Any withdrawals by relatives of the deceased are implemented in the same way as during the participant's lifetime. Is this correct and legally permissible?

The applicability of the GDPR to the information of a person ends with the death of that person.[38] Recital 27 of the GDPR explicitly states:

> *"This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons."*

The opening clause contained in the second sentence was only used in Germany, as far as can be seen, for the area-specific data protection law in accordance with § 35 SGB I in conjunction with Sections 67–120 SGB X. Section 35 para. 5 SGB I stipulates that the processing of social data is permissible if the provisions of Chapter 2 of SGB X are observed. In addition, however, the processing of the data is always permissible if no legitimate interests of the

38 *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 39.

deceased or his/her relatives are impaired by the processing. Social data are personal data which are processed by a body mentioned in §§ 35 SGB I with regard to its duties under the SGB (§ 67 para. 2 s. 1 SGB X).

The bodies mentioned in § 35 SGB I essentially include health insurance funds and associations of GKV-accredited physicians, but not health care providers, hospitals and research institutions. Only in the exceptional case that a research institution conducts research for a body named in § 35 SGB I and receives social data for this purpose, could the applicability of §§ 67–120 SGB X be considered according to § 35 Para. 5 SGB I.

As a rule, however, the basic rule will remain that the applicability of data protection law ends with the death of a person. However, this does not mean that all legal protection is no longer applicable upon death. In the context of the constitutionally guaranteed fundamental rights, one would no longer speak of a right to informational self-determination, but of a right to post-mortem personal rights. According to German constitutional law, the protection of post-mortem personal rights is based on the protection of human dignity, which extends beyond death. However, this protection does not extend to the general freedom of action under Article 2 para. 1 GG, which can only be exercised by the living.[39]

In its judgment of 12 July 2018, the Federal High Court (Bundesgerichtshof—BGH) ruled that, in the event of the death of the account holder of a social network, the contract of use is in principle transferred to the account holder's heirs in accordance with Section 1922 BGB.[40] Access to the user account and the communication contents contained therein are not opposed by the deceased's post-mortem personal rights, telecommunications secrecy or data protection law. However, the BGH left open the question as to whether a relative or heir may also assert data subjects' rights under data protection law. In the opinion expressed here, this is not the case. Only the data subject is entitled to data subject rights. Art. 4 No. 1 first half sentence GDPR defines the data subject as the identified person to which the data relate. They therefore constitute highly individual rights. The BGH concludes an authorisation to the access to a Facebook account by heirs not on basis of concerning rights after the GDPR, but alone from the fact that contracts, which a deceased had concluded, pass on to the heirs and the latter thus themselves become contracting partners. Aspects of data protection law are only examined by the BGH to the extent that it is established that data protection law does not preclude access by heirs.[41]

The BGH stated that in the event of an encroachment on the immaterial components of the post-mortem personal right, the closest relatives of the deceased

39 *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 39.
40 ECLI:DE:BGH:2018:120718UIIIZR183.17.0.
41 ECLI:DE:BGH:2018:120718UIIIZR183.17.0, Rn. 64.

may assert defensive rights in the form of injunctive relief and revocation claims.[42] However, if data continues to be processed for purposes for which the deceased had given his effective consent during his lifetime, no averting interference with post-mortem personal rights can be foreseen.

From a legal perspective it is therefore not mandatory to grant a right of withdrawal to the relatives. However, there should be no major obstacles to such a procedure.

42 ECLI:DE:BGH:2018:120718UIIIZR183.17.0, Rn. 53; BGH Urt. v. 6.12.2005 — VI ZR 265/04, BeckRS 2006, 808.

12 Studies within the European Union

As UMG has faced denial of transmission of personal data from participating hospitals in several European countries by virtue of legal obstacles, we have asked six partner law firms in European countries (Italy, Poland, Portugal, Serbia, Slovenia, Spain) to deliver a legal opinion on their national data protection regulations regarding the processing of personal data for the purpose of scientific research. In detail (cf. tab. 2), the first question aimed to see if the transmission of IDAT and documents containing IDAT to a central register in Germany is restricted by national regulations beyond GDPR (**1.**). Secondly, the question was asked whether in certain situations IDAT cannot be transferred to the central register in Germany despite the consent given by the patient and for legal reasons beyond GDPR (**2.**).

The legal information provided by the partner law firms dates from December 2018 and January 2019. In all relevant countries, the transposition of GDPR provisions into national law is still in progress. In principle, legal adjustments can be made at any time. In case of a specific research project in one of these countries, we therefore recommend reviewing the national regulations of the respective country.

Tab. 2 Legal opinions on national data protection regulations regarding the processing of personal data for the purpose of scientific research from Italy, Poland, Portugal, Serbia, Slovenia and Spain

	1. Regulations regarding the transmission of IDAT to a central register (beyond GDPR)		2. Particular use cases of illegal transfer from IDAT to Germany despite the consent of participant (beyond GDPR)	
Country	**Regulatory Requirements**	**Level of restriction[43]**	**Regulatory Requirements**	**Level of restriction**
Italy	■ No additional restrictions identified. ■ Italian Data Protection Authority confirmed the compatibility of the "General Authorisation to process of personal data for scientific research purposes" and the "Deontological Rules concerning the process of personal data for scientific research purposes" with the GDPR. ■ To date, no specific measures for the conduct of clinical trials have been issued by the Italian Data Protection Authority.	*	■ No additional restrictions identified. ■ The Ethic Committees approve also the used forms of the declaration of consent; their approval may vary.	*
Poland	■ Restrictions possible if IDAT are qualified as data of "medical records" (if surnames, first names, dates of birth, gender, address or place of residence, social security numbers, identification of the healthcare providers or description of the patient's health are contained). ■ Without the patient's consent, "medical records" data can only be transferred to universities and research institutes, but IDAT shall not be included. If the patient's consent has been obtained, IDAT can be transferred.	**	■ Additional restrictions identified. ■ In case of "medical record" data, the purposes of processing IDAT shall be clearly defined in the patient's declaration of consent. ■ In case of a "significant experiment", a prior positive voting of a Bioethics committee is required. ■ Depseudonymization may be inadmissible.	**

43 The following visualizations stand for: * no additional restrictions identified; ** additional restrictions identified; *** transmission of IDAT illegal in certain cases

	1. Regulations regarding the transmission of IDAT to a central register (beyond GDPR)		2. Particular use cases of illegal transfer from IDAT to Germany despite the consent of participant (beyond GDPR)	
Country	**Regulatory Requirements**	**Level of restriction[43]**	**Regulatory Requirements**	**Level of restriction**
Portugal	■ No additional restrictions identified. ■ The Ethics Committees approve the clinical trial by a risk-benefit-evaluation, taking into consideration also the used forms of the declaration of consent; their approval may vary. ■ The sponsor of the clinical study is responsible for compliance with the legal requirements for processing IDAT.	*	■ Additional Restrictions identified. ■ Information security regulations to be complied with. ■ IDAT have to be processed by persons subject to a legal obligation of professional secrecy.	**
Serbia	■ No additional restrictions identified. ■ The Ethics Committee and the Commissioner for the Protection of Personal Data approve the used forms of the declaration of consent and the export of IDAT; their approval may vary. ■ The intended processing of IDAT (e.g. manner of processing) and the declaration of consent (e.g. exact number and names of persons IDAT are disclosed to) have to be described precisely.	*	■ Additional restriction identified. ■ Export of IDAT to a country that is not a signatory to the Convention on the Protection of Individuals with regard to the automatic processing of personal data of the Council of Europe is illegal.	***
Slovenia	■ No additional restrictions identified. ■ IDAT cannot be transferred by physically transferring the original medical records or documentation being part of the original medical record.	*	■ No additional restrictions identified. ■ Physical transfer of original medical records or documentation being part of the original medical record cannot be consented to.	*

	1. Regulations regarding the transmission of IDAT to a central register (beyond GDPR)		2. Particular use cases of illegal transfer from IDAT to Germany despite the consent of participant (beyond GDPR)	
Country	**Regulatory Requirements**	**Level of restriction[43]**	**Regulatory Requirements**	**Level of restriction**
Spain	■ Additional restrictions identified. ■ The Ethics Committees approve the processing of pseudonymised data for research purposes; their approval may vary. ■ Access to pseudonymized data by TTP requires a confidentiality agreement. ■ De-pseudonymisation permitted only under certain conditions.	**	■ No additional restrictions identified.	*

13 Storage limitation

Clinical research projects funded by the DZHK take place in the public interest and the measures required by Art. 89 GDPR to protect data (separation of powers, data minimisation, pseudonymisation, anonymisation) are implemented. Storage for an indefinite period is essential for the collection of data and biomaterials to be used beyond the study period.

Are the storage and use of personal data and research data still permissible for an indefinite period of time after the data subject has been informed about this and has consented accordingly?

As a rule the GDPR does not allow infinitely long storage of data on stock. In article 5 GDPR, that formulates the essential principles of the data processing, it is said under lit. e) that personal data shall be

*"kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored **for longer periods** insofar as the personal data will be processed solely for archiving purposes in the public interest, **scientific** or historical **research** purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')" [Highlighting not in the original text]*

The right to erasure and right to be forgotten correlating with the principle of the storage limitation is laid down in Article 17 GDPR. As already explained above under Part II.3.2, personal data are to be erased according to the provisions of the Article 17 para. 1 GDPR if not one of the exceptions according to Article 17 para. 3 GDPR comes into play. Thus Article 17 para. 3 lit. d) GDPR states that the right to erasure and the right to be forgotten according to Article 17 para. 1 and 2 GDPR are not to be applied if the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 para. 1 GDPR in so far as the right referred to in Article 17 para. 1 GDPR is likely to render impossible or seriously impair the achievement of the objectives of that processing.

This would still mean, that in these cases, however, the data must be deleted immediately after the goal has been achieved.[44]

As the GDPR only allows storage for **longer periods**, but does not provide a maximum storage period, there is controversy as to whether the examination, whether the further storage is necessary for these purposes, can be waived[45] or not.[46]

According to the view expressed here, a potentially infinite storage can theoretically result as an exception to the principle of storage limitation, especially in the case of a broad consent. In order to avoid uncontrolled data retention, however, regular checks should also be carried out in the case of a broad consent to determine whether the purpose has been achieved. If, for example, one assumes that a disease to be investigated after broad consent is considered cured or that a research institution decides that no more research is to be carried out in a certain area (e.g. clinical trials of medicinal products), then a purpose may have been achieved or erasure may be necessary because a purpose has been abandoned.

How is the retention period of consent and research data defined by the GDPR?

GDPR does not define retention periods of consent and research data. However, retention obligations may result from technical legislation of the European Union or the Member States depending on the type of research project.

Is it advisable to secure the storage period of the data and the consents by the consent itself?

Yes, since consent must be informed in order to be effective, it must cover all essential aspects. This would also include a potentially infinitely long storage period in the case of a broad consent. It is not necessary to indicate that the consent form itself will be kept for as long as the research continues.

44 Koch/Schütze/Spyra/Wefer, in: Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS), Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Data protection requirements for medical research, taking into account the EU General Data Protection Regulation (GDPR), 16 May 2017, p. 35.

45 Kühling/Buchner/Herbst, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 69.

46 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 162.

14 Purpose limitation

At present, the study consent also allows the use and transfer of personal data for biomedical research projects. The consent is obtained without the possibility to exclude this purpose. According to Art. 5b) GDPR "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes".

Can further processing for purposes other than the study purpose (but nevertheless within the framework of research) be carried out in accordance with consent?

The GDPR permits a broad consent, which does not have to be limited to a specific research project anymore. A processing of personal data for several research projects, which are covered by this broader understanding of purpose limitation, can therefore take place on basis of the same declaration of consent, provided that it was formulated in conformity with the law and was obtained effectively. For this purpose it is particularly important that the essential information for a declaration of consent is still correct; for example, the data may not be processed by a new data controller.

It may however be a difficult question in individual cases whether a broad consent still meets the requirements of the principle of purpose limitation. The central prerequisite for effective consent is its specificity. A blanket con-

sent clause, which is not limited to specific data processing purposes, will as a rule be ineffective. On the other hand, consent does not have to be limited to a single data processing purpose. Article 6 para. 1 lit. a) and Article 9 para. 2 lit. a) GDPR explicitly state, that the data subject can give consent "for one or more specific purposes". Admittedly, the purpose must in principle be as precise as possible at the time of data collection and it must be ensured that personal data are not processed for purposes which the data subject did not have to expect at the time of collection.[47] But at the same time recital 33 GDPR states, that it should be possible for data subjects to give their consent for **certain areas of scientific research** and not only for specific research projects anymore. This is intended to address the problem of science that the purposes of data processing in the field of scientific research often cannot be fully stated at the time of data collection.

This, however, raises the question of what is meant by "certain areas of scientific research". In the explanatory memorandum on the reform of the Tenth Book of the German Social Code (SGB X) the German legislator made it clear that it also adheres to the main features of the specific consent pursuant to Art. 4 No. 11 DS-GVO within the Broad Consent framework and does not, for example, permit the obtaining of a universal consent.[48] For example, a reference to research purposes in general ("open consent") does not satisfy the principle of specificity even in the context of Broad Consent.[49] At least the research area must be explicitly defined beforehand. Accordingly, the legislator demands that the research area must not be too general and must refer to a thematically defined field which is gradually concretised.[50] However, it is not clear from the explanatory memorandum how narrow the thematically defined research area must be in detail and whether the person concerned must be informed about the concretisation. However, Article 13 para. 1 lit. c) and Art. 14 para. 1 lit. c) GDPR stipulate that the data subject must be informed of the "purposes of data processing". The information must be specific enough to enable the data subject to form a clear picture of which data are processed and for what purpose. There are good reasons why the broad formulation "biomedical research projects" still falls within the scope of broad consent. This represents the current status of interpretation of "broad consent" by the Medizininformatik-Initiative and has some likelihood to be accepted in the still ongoing process of alignment with the data protection authorities.[51]

The question whether Article 5 para. 1 lit. b) second half-sentence GDPR is to be applied, arises only in the context of an examination of the compatibility

47 Kühling/Buchner/Buchner/Petri, 2. Aufl. 2018, DS-GVO Art. 6 Rn. 178–180.
48 BT-Drs. 18/12611, S. 113.
49 *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 6 Rn. 9.
50 BT-Drs. 18/12611, S. 113.
51 https://www.medizininformatik-initiative.de/sites/default/files/2019-05/MII_AG-Consent_Einheitlicher-Mustertext_v1.6a.pdf

of the purposes according to article 6 Abs. 4 GDPR. This would be the case, if the new research project would fall outside the scope broad consent and therefore outside the scope of "biomedical research projects". Since the processing of personal data in this case would be based on consent, the interpretation must first and foremost correspond to the wording of the consent. A limitation resulting from the wording cannot be circumvented by the general interpretation rule of Article 5 para. 1 lit. b) second half-sentence GDPR. This rule of interpretation does not mean, moreover, that purposes of scientific research are always compatible with the original purpose, but are not per se incompatible with the original purpose, taking into account Article 89 GDPR.

15 End of a project

At the end of project funding (BMBF, DFG), TTP and IDAT remain in the "estate".

- *What must the relinquishing office ensure before IDAT is handed over?*
- *What must the receiving institution prove before the TTP transfers and deletes its data?*

Data protection law is not linked to the funding of research projects. It is therefore irrelevant to the question of how personal data is to be handled at the end of a project whether a particular funding has been terminated. The decisive factor is whether a research project has been completed or discontinued. In this case, as a rule, personal data will no longer be needed and shall therefore be erased. If, on the other hand, a research project continues to be financed with other funds, this would only have an effect on the question at hand if this would lead to a change in the bodies involved.

There may, however, be necessities to further process personal data in both cases. There may be other legal grounds that allow the processing for archiving purposes or quality assurance purposes for the different fields of research. Special retention periods can be found for example in the medicinal products law as well as in medical devices law. However that cannot be answered in general, but has to be assessed on a case-to-case basis.

The Deutsche Forschungsgemeinschaft (DFG) has published guidelines for the handling of research data, which states that according to the rules of Good Scientific Practice, research data should be archived for at least 10 years in the own institution or in a scientifically relevant, supra-regional infrastructure.[52] However, data protection requirements take precedence over the guidelines. In many cases IDAT will not be necessary in order to review and assess the validity of data and the quality of scientific work which would be the aim of the recommendation of the DFG. To maintain research possibilities it would be possible to delete name and birth date, converting the latter to an age group, and delete the address converting into assignment to an administrative district.

The idea that data must be returned after processing comes from a time when physical media had to be moved from one place to another and there was a legitimate interest in data recuperation. However, if data is not physically moved from one place to another nowadays, but only electronically duplicated, such a legitimate interest in retrieving data rarely still exists. However, if the sponsor or the person responsible for a research project has an obligation to retain certain data that he does not already have, this data would have to be transferred to him. Otherwise, erasure by the TTP would be sufficient on a regular basis.

- *What is normal/usual/allowed at the end of a project, if the erasure of the data is not forced by consent/study protocol ... for example in clinical epidemiological projects? Can the TTP switch off the services but continue to store the data without an ongoing project? Under what conditions?*

Erasure does not have to be forced explicitly by the wording of a consent form because the duty to erase data derives according to the provisions in Article 17 GDPR anyway.

Data storage is a form of data processing. It does not make a difference in this respect if a specific service is switched on or off. Data may be stored under the same conditions as the previous processing was allowed.

- *How long after the end of the project must the storage of a) consents and b) research data be ensured, unless otherwise specified?*

There is no general rule as to how long consent forms or research data must be stored. Consent forms may be stored at least as long as the processing of data continues and the principle of accountability demands that a controller shall be able to prove that a data subject has consented. More concrete provisions can be found in specific laws covering different fields of scientific research.

52 Deutsche Forschungsgemeinschaft, Leitlinien zum Umgang mit Forschungsdaten, Stand 30.09.2015, p. 1; http://www.dfg.de/download/pdf/foerderung/antragstellung/forschungsdaten/richtlinien_forschungsdaten.pdf.

- *Is it possible to transfer MDAT and/or IDAT to third parties after the end of the project?*
- *Under what conditions is the transfer of TTP data (Identifying Data [PII], pseudonyms + mappings, consents and withdrawals) to third parties permissible after the end of the project?*
- *Under what conditions is the transfer of research data to third parties permitted after the end of the project?*

MDAT may be transferred if it can be considered to be anonymous according to recital 26 of the GDPR[53] from the perspective of the receiving third party. In other cases the transfer of MDAT as well as IDAT must be lawful and would require to be covered by consent or another legal basis. There is no systematic difference as to other processing of personal data.

- *Who is responsible for checking the suitability of the third party as data trustee/processor?*

The controller is responsible for ensuring the suitability of a processor.

53 See Part I.2.2.2

16 Possession and ownership of data

Who is the data possessor, the data owner and the data processor in the context of the data processing described?

How do these terms exactly differentiate themselves from each other?

16.1 "Dateneigentum"/"data ownership"

The German term "Dateneigentum" ("data ownership") does not exist in legal jargon. In Germany the term for property ("Eigentum") always refers to "corporeal objects" (cf. §§ 90, 903 BGB). Data and information do not belong to these objects. For the described scenario it follows that there is no data ownership (in the sense of "Dateneigentum"). Rather, the classification and protection of intangible assets in the form of data and information is governed by intellectual property law (including copyright law and patent law).

16.1.1 Copyright and Copyright related rights

The German copyright law protects authors of works, that are the author's own intellectual creations (§ 2ff. UrhG), in their intellectual and personal relationships to the work and in respect of the use of the work (§ 11 UrhG). Protected works could be literary works, such as written works and computer

programs (§ 2 [1] Nr. 1 UrhG), illustrations of a scientific or technical nature (§ 2 [7] UrhG) or collections and database works (§ 4 UrhG).

Databases are additionally protected by a "related right" ("Verwandtes Schutzrecht"). According to § 87b UrhG the producer of a database has the exclusive right to reproduce and distribute the database as a whole or a qualitatively or quantitatively substantial part of the database and to make this available to the public.

Data of the participants of studies (for example name and address) and pseudonyms are no intellectual creations pursuant to § 2ff. UrhG. Furthermore, the data as such is no database (cf. § 87a UrhG).

The copyright protection of the consent form and of the quality reports depends on the human influence on the creation of the respective text or visualisation. In order to fall within the scope of protection of copyright, the the consent form and the quality report must be sufficiently original and individual.

16.1.2 Patent law

Legal protection by patent law requires an invention in a field of technology (cf. § 1 [1] PatG). Programms for computers and presentations of information are excluded from patentability to the extent to which protection is being sought for the subject-matter or activities referred to as such (§ 1 [3], [4] PatG). The Patentability of computer-implemented inventions is highly controversial.

16.1.3 Data protection law

The General Data Protection Regulation uses the term "own" in the context of a natural person's "own" data (recital 7: "Natural persons should have control of their own personal data"; cf. recital 68: "To further strengthen the control over his or her own data, [...] the data subject should ..."). The information about the participants of the studies (i.a. name and address) are personal data (cf. Art. 4 [1] GDPR).

16.2 "Datenhalter"/"data holder"/"data possessor"

The terms "data holder" and "data possessor" are used neither in intellectual property law nor in European data protection law.

16.3 "Datenverarbeiter"/"data processor"

The General Data Protection Regulation defines the terms "processing" (= Verarbeitung) in Art. 4 (2) GDPR and "processor" (= Auftragsverarbeiter) in

Art. 4 (8) GDPR. For the purposes of the GDPR 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art. 4 [8] GDPR).

The "processor" (Art. 4 [8] GDPR differs from the "controller" [= Verantwortlicher]). For the purpose of the General Data Protection Regulation "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

17 Data Protection Management System

Art. 5 and 24 GDPR demand the establishment of a data protection management system (DPMS).

Although GDPR does not state explicitly that a DPMS has to be installed, it is commonly agreed that a DPMS will serve the purpose of demonstrating that processing is performed in accordance with the GDPR.

Who is responsible for this establishment of a DPMS? (Designated data protection officer?)

The controller is responsible to fulfil the duties of accountability and thus the duty to demonstrate compliance with the GDPR. The tasks of a data protection officer are laid down in Article 39 GDPR. It is not the genuine responsibility of the data protection officer to establish a DPMS. However Article 39 para. 1 (b) GDPR states that it is one of the tasks of the data protection officer to monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.

As Monitoring is one of the main aspects of a DPMS it may however be advisable to entrust the task of establishing a DPMS to the data protection officer. It is legally permissible to assign further tasks to the data protection officer since the wording of Article 39 only defines the minimum number of tasks ("The data protection officer shall have at least the following tasks:").

> *The specifics of the Data Protection Management System are not comprehensively described in the GDPR. Can the drafting and review of a data protection concept or a legal opinion be regarded here as the implementation of a Data Protection Management System?*

No. A data protection management system is characterised by the fact that it ensures continuous monitoring and adaptation of data processing processes. These follow the concept of a PDCA-cycle (Plan-Do-Check-Act). A one-off review, or obtaining a legal opinion, can be an important step in such an approach.

18 Privacy by Design

Art. 25 GDPR demands "Privacy by Design". The trustee approach includes (cf. [Bialke, et al., 2015]):

- *informational separation of powers*
- *separation of IDAT and MDAT*
- *use of ID management according to the Master Patient Index concept for record linkage*
- *use of pseudonym management*
- *digital consent management and modular Informed Consent approach*
- *workflow-controlled TTP dispatcher approach for overarching complex TTP workflows*

Is the trustee approach presented suitable for implementing the goals of Privacy by Design?

The principle of privacy by design is introduced for the first time under EU law in Article 25 GDPR. It means that data protection is realised through or with the help of technology and organisation. The aim is to develop data protection-friendly systems that do not allow data protection regulations to be disregarded. Data protection is inherent in such systems. privacy by design thus begins in the pre-processing phase. The fundamental rights of the data subjects are already protected by draft of the system.

Article 25 para. 1 of GDPR requires the controller to take technical and organisational measures to ensure compliance with the regulation and that the rights of the data subject are protected. With regard to the timing, the provision stipulates that these measures must be taken as soon as the purposes of the processing are determined, but also at the time of the processing itself. Concerning the suitability of the measure, the following factors have to be taken into account: The state of the art and implementation costs as well as the nature, extent, circumstances and purposes of the processing. The seriousness and probability of the risks to the rights and freedoms of natural persons arising from the processing must also be taken into account. As an example of the implementation of the data protection objectives from Art. 5 GDPR—such as that of data minimisation—and thus for an effective implementation of privacy by design, the provision names pseudonymisation in accordance with Art. para. 5 GDPR.

The measures that are taken in the Trusted Third Party approach to implement privacy by design seem to fulfil the requirements set out in Article 25 para. 1 GDPR from our point of view.

As a side note we point out that some stipulations of the GDPR in our opinion do not correspond to the principle of the certainty of laws. Laws must be in any case then very specific if a national authority shall be able to sanction a possible violation of the law. In our opinion the provision is too indefinite to be subject to fines by the data protection authorities. Should there be a violation of the principle of privacy by design, the risk of a fine may be estimated as low.

19 Use of eGK number or KV number

Are the electronic health card (eGK) and health insurance number (KVNR) particularly items worthy of protection in terms of data protection?

- *Under what conditions may the TTP collect/process these data, is an explicit consent (consent policy) necessary for this or can these items be processed as IDATs?*
- *Under what conditions may TTP use this data for matching (determination of a person's identity)? (ID with wide scope for merging data)*

19.1 General Information on the eGK and the KVNR

Each health insurance fund issues an electronic health card (eGK) for each insured person, which serves as proof of entitlement to benefits within the scope of GKV-accredited medical care (proof of insurance) as well as billing with the service providers (Section 291 para. 1 S. 1, 2 SGB V). The health insurance number (KVNR) is printed on the electronic health card (Section 291 para 2 S. 1 Nr. 6 SGB V).

The KVNR is defined in Section 290 SGB V. It consists of an unchangeable part for the identification of the insured person and a changeable part which contains nationwide information on the affiliation to the Fund and from which it must be ensured when assigning the number to the insured person that the reference to the relative who is a member can be established (Section 290

para. 1 S. 2 SGB V). The structure and procedure for assigning the health insurance number are regulated in the guidelines of the Central Association of Health Insurance Funds (GKV-SV), Section 290 para. 1 S. 3, Para. 2 S. 1 SGB V.

"To prevent the creation of a personal indicator that is valid across several branches of the social insurance system"[54] the pension insurance number may not be used as a KVNR, but may only be derived retroactively from it. However, it was precisely the purpose of the regulation to "create a permanent identification feature in the telematics infrastructure system"[55] with the unchangeable part of the KVNR.

19.2 Special legal significance of an unchangeable identifier

The risk potential of unchangeable personal identifiers lies in the possibility of linking different databases so that comprehensive personal profiles could be created. These considerations are based, inter alia, on the decisions of the Federal Constitutional Court (BVerfG) on the microcensus and the population census. In the microcensus resolution, the BVerfG said:

> *"It would not be compatible with human dignity if the state could claim the right to compulsorily register and catalog the person in his or her entire personality, even in the anonymity of a statistical survey, and thus treat him or her as a matter that is accessible to an inventory in every respect."*[56]

In the census judgment, the BVerfG also stated that a complete or partial registration and cataloguing of the personality was incompatible with human dignity under Article 1 para. 1 of the German Constitution (Grundgesetz—GG). It said, that this may be the case if

> *"(...) an unrestricted linking of the collected data with the partly very sensitive data stocks available at the administrative authorities or even the indexing of such a data network by a uniform personal identifier or other regulatory feature would be possible; because a comprehensive registration and cataloguing of the personality by the combination of individual life data and personal data for the compilation of personality profiles of the citizens is also inadmissible in the anonymity of statistical surveys."*[57]

The introduction of a uniform personal identification mark was therefore "a decisive step towards registering and cataloguing the individual citizen in his

54 BT-Drs. 15/4924, S. 8.
55 *Hornung/Roßnagel* in: Schneider, Sekundärnutzung klinischer Daten—Rechtliche Rahmenbedingungen, 2015, S. 395.
56 BVerfGE 27, 1 (6).
57 BVerfGE 65, 1 (53).

or her entire personality"[58] and, according to this opinion, should be constitutionally inadmissible.[59] However, as long as serial numbers, e.g. passport or ID card numbers, are only used for one purpose or for manageable purposes, they are considered permissible.[60] The BVerfG has also not universally and unconditionally rejected the introduction of personal identifiers; a constitutional design would be conceivable through organisational, technical and legal measures.[61]

The problem of a uniform personal identification number is also addressed in Art. 87 GDPR. Accordingly, there is an opening clause in favour of the Member States concerning the processing of a national identification number or other marks of general importance. Member States may allow processing by national law, but must provide appropriate safeguards for the rights and freedoms of the data subject. In Germany there are no national identification numbers and the sectoral personal identifiers, such as the KVNR, are not of "general significance" within the meaning of Art. 87 GDPR; they are therefore subject to general data protection law.[62]

19.3 Additional sensitivity as a Data about health?

With regard to the KVNR, it could be considered that this is already data concerning health, as recital 35 states:

> *"Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.*
>
> *This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (9) to that natural person;* ***a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes;*** *information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data*

58 BVerfGE 65, 1 (57).

59 *Polenz* in: Kilian/Heussen, Computerrecht, 33. EL Februar 2017, 1. Abschnitt. Erläuterungen Teil 13: Datenschutz Verfassungsrechtliche Grundlagen des Datenschutzes Rn. 18–21

60 *Polenz* in: Kilian/Heussen, Computerrecht, 33. EL Februar 2017, 1. Abschnitt. Erläuterungen Teil 13: Datenschutz Verfassungsrechtliche Grundlagen des Datenschutzes Rn. 20.

61 *Martini/Wagner/Wenzel*, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017, S. 62; with the correct remark that the technical possibilities of BigData applications relativize the importance of personal identifiers, since profile formation can also take place on the basis of many different data records. see regarding the tax numbers: FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08.

62 BeckOK DatenschutzR/ von Lewinski, 23. Ed. 1.2.2018, DS-GVO Art. 87, Rn. 53.

> *subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test." [Highlighting not in original text]*

Thus, identification markers in themselves would also represent health data, although they do not necessarily provide information about the state of health. However, the meaning of recital 35 is unclear. This extensive understanding of the concept of health data has not been reflected in the text of the Regulation: The wording of Article 4 No. 15 GDPR defines data concerning health on as:

> *"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;"*

An interpretation according to the solely relevant wording of the standard text as well as an interpretation according to systematics, sense and purpose, however, argues against an extension of the definition of data concerning health to identifying characteristics which do not contain any health-related meaning. We therefore are of the opinion that the processing of the KVRN does not qualify as processing of data concerning health.

19.4 Non-validated issuing process

It should be noted that the creation and distribution of the electronic health card is error-prone and the card cannot be securely attributed to a natural person.

The issuance of the eGK is regulated in § 15 Para. 6 SGB V, according to which the health insurance funds are to counteract the misuse of the card by appropriate measures.

While the law demands, that the eGK must be signed by the insured person, Section 291 Para. 1 S. 4 SGB V, and that it must also bear the photograph of the insured person Section 291 Para. 1 S. 4 SGB V,[63] it is not expressly regulated in the law how the health insurance funds ensure that the picture provided is actually one that shows the insured person or how the information provided by the insured person, for example within the scope of reporting the data in accordance with § 10 Para. 6 SGB V, is validated. Likewise, the manner in which the card is issued is not prescribed. In contrast to identity documents such as identity cards or passports, electronic health cards are not issued in a personal handover process, but are sent by mail. Although this procedure is

63 However, an electronic health card without a photograph must be issued for insured persons up to the age of 15 and for those whose participation in the creation of the photograph is not possible (Section 291 Para. 2 S. 5 SGB V).

not demanded by law as a mandatory procedure, it is considered permissible in any case (cf. Section 291a Para. 3 S. 3 SGB V: "when sending the card").

The non-validated process was dealt with in a so-called "small inquiry" to the Federal Government. The Federal Government replied that the health insurances are responsible for the issuing process of the eGK and that a sufficient identification of the insured persons would be ensured by the statutory reporting provisions in according to Section 5 Para. 5 Ordinance on the Collection and Transmission of Data for Social Insurance Institutions (Data Collection and Transmission Ordinance—DEÜV) upon entry into the statutory health insurance system. According to this provision, the personal details reported to the social insurance institutions are to be taken from official documents. This obligation on the part of those obliged to register under Section 2 DEÜV, for example the employer, is sufficient for sufficient identification. The Federal Government did not consider further identification to be necessary as the eGK was not an identity document such as a passport or identity card. Such an obligation would not arise from Section 291 SGB V either.

Furthermore, it cannot be assumed that incorrect data will be discovered and corrected during a visit to the physician, as there is no obligation for health care providers to compare the eGK with an identity card. Only obvious errors that can be identified on the basis of the identity data applied to the eGK (photograph, signature, surname, first name, date of birth) are to be checked by GKV-accredited physicians, cf. No. 1.2. of Appendix 1 to § 7 of Annex 4a Federal Master Treaty for Medical Practitioners (Bundesmantelvertrag Ärzte—BMV-Ä).

19.5 Special restrictions of use according to the SGB V

In the past, the use of the health insurance card (KVK)[64] and the KVNR for research purposes had been argued on the basis of Section 291 SGB V in its version valid until 28.12.2019.[65] Thus it was argued that the regulation of Section 291 para. 1 sentence 3 SGB V (old version) prescribed a strict purpose limitation of the eGK as well as the KVNR as proof of insurance and means of settlement. The provision read as follows until 28.12.2015:

> *"With the exception of § 291a, it [the health insurance card] may only be used as proof of entitlement to claim benefits within the framework of GKV-accredited physicians and for invoicing with the health care providers."*[66] *[Addition in brackets was added by the authors]*

64 This was the previous version of the eGK.

65 *Hornung/Roßnagel*, in: Schneider, Sekundärnutzung klinischer Daten—Rechtliche Rahmenbedingungen, 2015, p. 367–404.

66 "Sie darf vorbehaltlich § 291a nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden."

This regulation was regarded as conclusive and, with reference to a judgment of the Federal Social Court of 10 December 2008, it was then concluded that processing of the KVNR could not be justified by consent either, since recourse to general data protection laws was not possible.[67] The Federal Social Court had ruled that billing data according to the SGB V may not be passed on by health care providers to private service providers for billing purposes.[68] Furthermore, it was argued that the extended usage possibilities of the eGK according to Section 291a SGB V (old version) were not sufficient, since Section 291a para. 8 SGB V excluded a consent with justifying effect.[69]

By reforming Sections 291 and 291a SGB V as of 29 December 2015, the strict wording "only" was replaced with the following wording:

> *"It [the eGK] serves as proof of the entitlement to claim benefits within the framework of GKV-accredited physicians (proof of insurance) as well as the settlement with the health care providers." [Addition in brackets was added by the authors]*

The wording of the law therefore no longer excludes any other use of the eGK.

In addition, Section 291a Para. 7 S. 3 SGB V includes a provision on health research. This allows the use of the telematics infrastructure cure for purposes of health research under certain conditions. According to the explanatory memorandum, this provision is intended to enable the use of the telematics infrastructure without the use of the eGK. However, the use of the eGK for research purposes is not permitted by this provision.

Regarding the rulings of the Federal Social Court, which was already criticised under the old legal position of the data protection guideline,[70] now from a substantial change by the validity acquisition of the GDPR might be to be assumed. In relation to the national law, e.g. the SGB V, the GDPR prevails. Only in the context of Article 9 para. 2 lit. a) GDPR the possibility to consent to the processing of data concerning health can be excluded by the member states. The statement of the Federal Social Court, that there is no principle after which one could fall back on the possibilities of giving consent as provided by general data protection law cannot continue to apply under the general data protection right without further ado. In order for the opening clause of Article 9 para. 2 lit. a) GDPR to be used in conformity with EU law, consent would have to be expressly excluded. This is precisely not the case if the possibility to con-

67 *Hornung/Roßnagel*, in: Schneider, Sekundärnutzung klinischer Daten—Rechtliche Rahmenbedingungen, 2015, p. 400.

68 *BSG*, Urteil vom 10. Dezember 2008—B 6 KA 37/07 R—, BSGE 102, 134–148, SozR 4-2500 § 295 Nr. 2.

69 *Hornung/Roßnagel*, in: Schneider, Sekundärnutzung klinischer Daten—Rechtliche Rahmenbedingungen, 2015, p. 40380.

70 *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, p. 176; *Heberlein*, SGb 2009, 717; *Brisch/Laue*, CR 2009, 465; *Schneider*, VSSR 2009, 381; *Leisner*, NZS 2010, 129; *Kingreen/Temizel*, GesR 2010, 225; *Kühling/Seidel*, GesR 2010, 231; *Hauser*, KH 2011, 910.

sent is assumed to be denied from the reverse conclusion that the legislator allowed consent only in those cases where he wanted to consent to happen and therefore wanted consent to be excluded where it was not expressly permitted.

It should be noted, that Section 291a para. 8 SGB V does not allow to demand Access to certain Data on the eGK nor to conclude an agreement on it. Any infringement of this provision may result in the imposition of a fine according to Section 307 Section 1 SGB V. Anyone who, contrary to Section 291a para. 4, s. 1 or para. 5a, s. 1, first half sentence or sentence 2 SGB V, accesses the data mentioned therein may be liable to prosecution according to Section 307b SGB V.

19.6 Conclusion

The following can be concluded from the above: The eGK and the KVNR are items particularly worthy of protection. However, the lawful processing of the KVNR for the purpose of scientific research is possible. SGB V does not conclusively regulate the use of the eGK and the KVNR and thus prohibit the processing for the purpose of scientific research. The processing of the KVNR could be performed on a legal basis or on the basis of consent, if this is necessary for the purpose of the processing. Additional consent for the KVNR would not be necessary. However, the "general" declaration of consent should indicate that the number is being processed. From a legal perspective, the question arises as to whether the use of KVNR is absolutely necessary. This has to be considered in the light of the non-validated issuing process of the eGK. In addition it is to be noted that with the use of the KVNR as additional date also additional errors can happen. The necessity of processing the KVNR must therefore be accurately assessed and the supporting reasons documented.

20 Technical and Organisational Measures (TOM)

Integrity and confidentiality belong to the key principles relating to processing of personal data. According to Article 5 para. 1 lit. f) GDPR this implies to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, which can be achieved by using appropriate technical or organisational measures. Technical and organisational measures play a role in different Articles within the GDPR, yet most importantly they have to be set up to ensure data security which is specified in Article 32 GDPR. Data security can be described as technical and organisational measures that prevent unauthorised handling of personal data. It thus serves to protect the fundamental rights of data protection and informational self-determination.

Since data protection laws first entered into force, attempts have been made to make technology subject to achieve data protection objectives. These correspond to the IT-Security objectives and are defined as availability, integrity and confidentiality. In recent years this was complemented by specifications for privacy by design. While the aim of privacy by design is to implement technical and organisational measures in the technology, technical and organisational measures that are subject to data security can be used at any time during the process of processing personal data. Technical and organisational meas-

ures that ensure data security shall prevent unauthorised handling of personal data.

Data security describes a situation in which the risk of damage to the fundamental right of protection of personal data is reduced to a minimum. Article 32 of GDPR as the central provision for data security is entitled with "Security of processing" and obliges both the controller and the processor to take appropriate measures to ensure secure processing. Article 32 GDPR substantiates the central principle of system security pursuant to Article 5 para. 1 lit. f) GDPR. Technical and organisational measures must ensure protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This includes that unauthorised persons have no access to the data and cannot use the data or the devices with which they are processed.

Pursuant to Article 32 para. 1 GDPR, controllers and processors are obliged to take appropriate technical and organisational measures to ensure a level of protection appropriate to the risk. In doing so, the state of the art, the implementation costs and the nature of the scope, circumstances and purposes of the processing as well as the different probability of occurrence and the severity of the risk for the personal rights and freedoms of natural persons must be taken into account. In its paragraph 1 the provision also entails a list, containing instruments, characteristics and procedural requirements, that can be used to ensure data security:

- the pseudonymisation and encryption of personal data (lit. a)
- the ability to secure the long-term confidentiality, integrity, availability and resilience of processing systems and services in connection with the processing of personal data (lit. b)
- the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident (lit. c)
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The GDPR follows a risk-based approach. The technical and organisational measures must always ensure a level of protection appropriate to the risk which means that the controller has to carry out a risk assessment on a case-by-case basis before each data processing operation and draw up an individually balanced protection concept.

Article 32 para. 2 GDPR specifies the risks to be taken into account when assessing the appropriate level of protection. These are, in particular, risks associated with processing, namely: unintentional or unlawful destruction, loss or alteration, unauthorised disclosure of or access to personal data. According to Article 32 para. 3 GDPR, an indication that the requirements set out in Article 32 para. 1 GDPR have been met may be compliance with an approved code

of conduct pursuant to Article 40 GDPR or a certification as set out in Article 42 GDPR.

The GDPR contains many opening clauses that allow the national legislator to enact national and subnational laws. A few of these opening clauses are set out in Article 9 para. 2 GDPR that authorises national legislators to enable processing of data concerning health and other special categories of personal data despite the fact, that processing of special categories of personal data is generally prohibited. The German Federal Data Protection Act made use of this and while it does not contain any general requirements for data security, it does contain requirements for the processing of special categories of personal data in Section 22 para. 2 BDSG. According to this Section, the following measures have to be provided in order to legally process data concerning health:

- Technical organisational measures to ensure that processing complies with the GDPR;
- Measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
- Measures to increase awareness of staff involved in processing operations;
- Designation of a data protection officer;
- Restrictions on access to personal data within the organisation of the controller and by processors;
- The pseudonymisation of personal data;
- The encryption[71] of personal data;
- Measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- Specific rules of procedure to ensure compliance with the German Federal Data Protection Act and with the GDPR in the event of transfer or processing for other purposes.

The Federal Data Protection Act (BDSG) also calls for the sensitisation of those involved in processing operations, the designation of a data protection officer and the restriction of access to personal data, as well as measures to enable subsequent verifiability of the processing operations, partly in the same spirit as and partly in addition to the measures required by the GDPR.

71 For example the BSI Guideline TR-02102 on Cryptographic procedures: Recommendations and encryption key lengths should be considered. BSI publications can be found under the following link: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

Both the provisions of the GDPR and of the German Federal Data Protection Act are rather general, which is why specific requirements cannot be derived from them. However, it is still possible to apply the annex to Section 9 BDSG sentence 1 (old version). The measures that are listed in the old version of the German Federal Data Protection Regulation can still be used to substantiate the requirements of Article 32 GDPR. Article 32 para 1 of GDPR contains a catalogue which presents "among other things" how technical and organisational measures can be designed. These include data security objectives as confidentiality, integrity and availability on the one hand and security measures to promote these objectives on the other. In contrast, the annex to Section 9 sentence 1 BDSG (old version) lists measures that are suitable for achieving data security. The term "technical and organisational measures" is to be understood broadly in the GDPR. Although it is not defined, technical and organisational measures are intended to serve very different purposes. For example to ensure fair and transparent processing of personal data within the framework of profiling or to ensure privacy by design as well as to guarantee data security.

The requirements and concepts for physical access control, electronic access control, transfer control, input control and data entry control as well as the separation requirements of the Annex to Section 9 sentence 1 BDSG (old version) can still be used under the GDPR as concrete measures to ensure the security of processing. The catalogue of Article 32 para. 1 GDPR is unstructured, random and above all not conclusive. The wording "inter alia" makes it clear that this is an exemplary list of measures, characteristics and procedural requirements that can be used to achieve the objective of data security. In addition, other measures can be used as long as they do not contradict the GDPR, but support its objectives. The security of data processing is set out as a central principle of processing in Article 5, yet the list of measures in Article 32 GDPR is rather sparse, which is why it can only be in line with the European legislator to implement further measures than those mentioned in Article 32 GDPR.

This leads to the conclusion, that the following measures (sorted by data security objectives that need to be achieved) have to be considered to assure data security—always appropriate to the risk and therefore assessed on a case-to-case basis:

- Confidentiality
  - Physical Access Control (Prevention of unauthorised access to data processing facilities)
  - Electronic Access Control (Prevention of unauthorised use of data processing and data storage systems)
  - Internal Access Control (Prevention of unauthorised copying, reading, alteration or deletion of data within the system)
  - Isolation Control (Prevention of processing data together that is collected for different purposes)
  - Pseudonymisation

- Integrity
  - Data Transfer Control (Prevention of unauthorised copying, reading, alteration or deletion of data while it is transferred)
  - Data Entry Control (Record of what and by whom is entered into a data processing system or altered or deleted)
- Availability and resilience
  - Availability control (Prevention of accidental or wilful destruction or loss of data)
  - Rapid recovery
- Procedures for regular testing, assessment and evaluation
  - Data protection management (e.g. SOP)
  - Incident response management (e.g. SOP)
  - Data protection by design and default
  - Order or contract control

This is in line with a guideline published by the German "Gesellschaft für Datenschutz und Datensicherheit e.V." (GDD), presenting and explaining necessary technical and organisational measures.[72]

For the data that is processed by the UMG which will mainly be data concerning health a high standard of data security will be necessary. However, we can not give specific advice on which technical and/or organisational measures need to be implemented as these are highly dependant on the state of the art and therefore are subject to constant change. Guidelines on these measures are published by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik—BSI).[73] Also, the data protection authorities are just beginning to pay attention to this topic.[74]

As part of the development of a data protection management system, regular reviews of the BSI publications and the publications of the data protection supervisory authorities should therefore be carried out. The effectiveness and adequacy of technical and organisational measures should be reviewed and, if necessary, adjusted as part of regular internal audits.

72 Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), GDD-Praxishilfe DS-GVO IV, Appendix; https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo.

73 For example the BSI Guideline TR-02102 on Cryptographic procedures: Recommendations and encryption key lengths should be considered. BSI publications can be found under the following link: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

74 The DSK publishes guidances which can be found at: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html.

21 Data usage by industrial partners

Which legal framework must apply if research data already covered by consent are to be used for secondary research and/or by industrial partners (e.g. for quality assurance of implants)?

The secondary use of personal data must be justified under data protection law following the same logic as in the case of primary use. In addition to GDPR, a large number of federal and state laws must also be taken into account in the case of additional research institutions and industrial partners. It is not possible to make a general statement about permissible further processing of personal data by other controllers and/or for other purposes. Depending on the controller and the purpose of the data processing, the applicable data protection law must be identified. Either the right to process data can be directly derived from the law, or the processing can be based on a consent.

If there is already a consent in place for the primary use of data this consent would have to cover also the secondary use of data. This may be a seldom situation as it would be particularly difficult to make sure that the new purpose of the secondary use is covered by the old consent and especially that the new controller is covered by the old consent.

As a rule it can be said that for further scientific research with existing personal data there will often be a legal basis that would allow the processing. In

such cases, information on further research must of course be provided according to Article 13, 14 GDPR.

On the other hand, there are usually no laws that permit the processing of health data for quality assurance purposes in commercial enterprises. Exceptions arise in particular for reasons of ensuring high standards of quality and safety of medicinal products and medical devices pursuant to Article 9 para. 2 lit. i) GDPR in conjunction with Section 22 para. 1 No. 1 lit. c) BDSG. It should be noted that there are more specific regulations in the AMG and the MPG, that would mostly cover the relevant cases. Accordingly, Section 22 para. 1 No. 1 lit. c) BDSG is viewed as not having its own relevant use case.[75] These regulations regularly cover the manufacturer, but not a TTP. A TTP could only be involved as a data processor without the consent of the person concerned.

It will, however, usually be possible to carry out quality assurance of products with anonymous or pseudonymous data. If this is the case, the processing of personal data would be inadmissible anyway, as is clear from the principle of data minimisation.

75 BeckOK DatenschutzR/Albers/Veit, 26. Ed. 1.5.2018, BDSG § 22 Rn. 14–17.

22 Necessity of documents

The GDPR requires the creation and maintenance of extensive documents and directories.

- *Which documents are legally mandatory according to the GDPR (e.g. data protection concept, description of procedure, list of procedures)?*
- *Is it legally necessary to carry out a data protection impact assessment? If so, please advise us on the (document) form, scope and level of detail of this data protection impact assessment.*
- *Which documents are mandatory for DFG- or BMBF-funded research projects and what can be stored if necessary?*

The GDPR demands various documents according to the principles of accountability and transparency. Some are explicitly listed in the GDPR. Others developed in practice as usual documents of value. To the latter data protection handbooks and whitepapers belong.

The GDPR demands a directory of the processing activities as central document whose requirements are listed in detail in Article 30 GDPR. This will be the core element of the data protection documentation, which can be merged into a comprehensive compendium. This is often referred to as a data protection manual or data protection concept. Furthermore information is to be provided according to Article 13, 14 GDPR compellingly. These are summarised usually in data protection declarations (also called a privacy policies) which can be

made available in different forms to the data subject and can also be added to the data protection manual.

Further it is to be proven that consent was given. Therefore consent forms should be achieved. The wording of such declarations could also be documented in the data protection manual.

Finally a data protection impact assessment is to be made according to Article 35 GDPR and to be documented accordingly. The instrument of data protection impact assessment is a new instrument of European data protection law. Until now, information from the data protection supervisory authorities is only available to a limited extent. A "best practice" has not yet been established in this respect, but the experience gained from initial approaches should be taken into account here. The data protection impact assessment is not a one-off review but an instrument of continuous analysis and further development in the sense of a PDCA cycle.

The following minimum requirements can be derived from the legal system of Art. 35 DS-GVO:

First of all, a threshold value analysis must be carried out on an expected high risk for the rights and freedoms of a natural person that may arise from the processing of personal data. Pursuant to Art. 35 para. 7 DS-GVO, a data protection impact assessment must include at least one processing directory (shortened to reflect any high risks). Accordingly, the necessity of data processing for a specific purpose (necessity and proportionality) must be explained. The third step is to assess the risks. Finally, appropriate corrective measures should be presented.

The Datenschutzkonferenz (DSK) has provided a paper on how to perform a data protection impact assessment called "Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen", dated 26 April 2018.

23 Responsible supervisory authority

Data subjects have the right to lodge a complaint with the responsible supervisory authority. This should be specified precisely in the consent. In the case of an EU-wide project: which authority is the responsible supervisory authority in this case?

The requirement to indicate the competent authority in a consent form does not exist according to the GDPR. Merely in Article 13, 14 GDPR it is demanded (as part of the duty to inform), that the controller has to inform about "the right to lodge a complaint with a supervisory authority" (Article 13 para. 2d) GDPR; Article 14 para. 2e) GDPR). It is nowhere to be found in the law, that the competent authority has to be specified.[76]

However, the competent authority will usually be the state data protection commissioner of the federal state in which the controller is located.

76 Gola/*Franck*, DS-GVO, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 24; BeckOK DatenschutzR/*Schmidt-Wudy*, 26. Ed. 1.11.2018, DS-GVO Art. 15 Rn. 71. Dissenting view: Kühling/Buchner/*Bäcker*, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 39.

24 Release from Obligation to Secrecy

What happens if the current consent form does not provide for an explicit release from the duty of confidentiality according to § 203 StGB?

Which test criteria can be used to determine algorithmically whether a release from the duty of confidentiality is required in a project?

Data protection law and secrecy obligations are instruments to be applied in parallel which represent a kind of double wall of protection (the so-called two-barrier principle). In accordance with Section 1 para. 2 sentence 2 BDSG the secrecy obligations remain unaffected by the BDSG. For the purpose of clarification, an identical provision has also been included now for social data protection law in § 35 Para. 2a SGB I.

The data protection law regulates the processing of personal data comprehensively according to the broad term of the processing in article 4 No. 2 GDPR and gives the data subject far-reaching powers of disposal over the data concerning it. The obligation to secrecy however regulates only the unauthorised disclosure of information in which a person could have a secrecy interest. Doctors are bound to secrecy as a result of the exercise of their profession. One can therefore refer to it as professional secrecy. Professional secrecy is regulated by the professional code of conduct of the physicians of the chamber district applicable to the respective physician, which is modelled following the requirements of the model professional code of conduct of physicians (MBO-Ä).

On the other hand, there is a criminal law form of confidentiality for some professions, which also include physicians in Section 203 StGB.

One way in which a secret may nevertheless be disclosed is if the person concerned declares his or her approval and therefore abandons the special protection of confidentiality. It would be wrong to say that a release from confidentiality is absolutely identical to consent under data protection law.[77] However, consent under data protection law to the transmission of personal data can at the same time legitimise the disclosure of secrets that are subject to a duty of confidentiality. If the data subject consents to the use of personal data (concerning health) for the purpose of scientific research and understands that data will not only be processed by a treating physician but also transferred to other scientists or for example a TTP, no further release from medical secrecy is mandatory. However, in order to take into account the principle of transparency and to allow informed consent, it is recommended that a consent text should include an indication that the consent also includes a limited disclosure of secrets. It may be important to note that the recipient of the data may no longer be protected against seizure.

A release from confidentiality will always be necessary if data are to be collected by a doctor or a hospital or transmitted by this without only anonymous data being affected.

In special constellations, it may not be necessary to release a physician from his duty of confidentiality with regard to a TTP if research is as an exception part of the physician's professional activity. As a general rule, this could be assumed in university hospitals. Then TTP employees could be legally involved in the secret as so-called "other persons involved". According to Section 203 para. 3 S. 2 StGB, physicians may disclose foreign secrets to other persons who are involved in their professional or business activities to the extent that this is necessary for the use of the activities of the other persons involved; the same applies to other persons involved if they make use of other persons who are involved in the professional or business activities of the aforementioned persons.

The doctors must then have ensured that any other person involved who discloses without authorisation a secret which has come to his knowledge in the course of or on the occasion of his duties has been obliged to maintain secrecy. Otherwise they are liable to prosecution.

77 Nevertheless with a dissenting view: Bieresborn, jM 2019, 41 (42).

25 Necessity of a contract on data processing

When does the GDPR require the conclusion of a contract on data processing?

Article 28 para. 3 s. 1 GDPR demands a data processing agreement whenever the processing of personal data is carried out by a processor on behalf of a controller. The aspects that are to be dealt with in a corresponding contract are also listed in Article 28 para. 3 GDPR.

It should be considered, however, that not every cooperation of two parties is to be regarded as data processing. In particular data processing must be distinguished from a joint controllership. For the latter also a contract is necessary, which is regulated in Article 26 GDPR.

In order to answer this question as well as the following questions, it is therefore necessary to clarify which bodies are controllers, processors or joint controllers. One body may be classified differently with regard to different data processing processes within the same research project. It would be conceivable, for example, that a TTP would carry out pseudonymisation as a data processor, but that consent management would be carried out under joint control.

The assignment results directly from the **actual circumstances** and the requirements of the GDPR. Article 4 No. 7 GDPR defines the "controller" as

> *"the natural or legal person, public authority, agency or other body which, **alone** or **jointly with others, determines the purposes and means of the processing** of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;" [Highlighting not in original text]*

By way of comparison, the data processor is defined as follows pursuant to Art. 4 No. 8 GDPR:

> *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"*

The decisive legal criterion for the distinction between controller and processor is the determination of the *purposes* and *means* of processing. Whoever determines purposes and means becomes a controller. If two or more jointly determine the purposes and means, they are considered joint controllers. If, on the other hand, one body carries out processing operations subject to instructions only, this body would have to be regarded as a processor. In individual cases it may be difficult to distinguish between a controller and a data processor. This applies in particular if one party does not determine both (purposes and means) or all parties determine both in unequal parts. Particularly difficult but frequent are cases in which either one determines the purposes and the other the means or both bodies can have a say in both points, but there is an imbalance.

The German legal literature lacks empirical values from the old legal situation, as the German legislator had not implemented the joint responsibility contrary to the wording of the Data Protection Directive (Directive 95/46/EC) and in the past only had to distinguished between controller and processor.

From this perspective, it can be said that the joint controllers are a new legal category. This has given rise to a variety of legal views.[78] For example, a minority opinion assumes that each of the joint controllers must always define both the purposes and the means and that this must be done equally balanced; at the same time, this opinion assumes that the "means" of processing are the data processed.[79]

In its decision of 5 June 2018 on joint responsibility for Facebook fanpages, the European Court of Justice contradicted a requirement of equally balanced determinations of both means and purposes.[80] Although this judgement still was based on the old legal situation under the Data Protection Directive, no

78 *Schreiber*, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden, ZD 2019, 55.
79 *Schütze/Spyra*, Art. 26 DS-GVO: Gemeinsam Verantwortliche, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V., Version 1.0 Stand: 17. 06. 2018, S. 5f.
80 *EuGH*. Urt. v. 05. Juni 2018, AZ: C-210/16. Rn. 38.

indications for a deviating assessment result in respect to the GDPR. With the prevailing opinion in legal literature it is to be held in addition that the **means** of the processing are not the processed data, that rather are the object of the processing, but the question of how a processing is accomplished.[81] This includes, in particular, data processing systems and processes. For example the means of processing include consent management systems, quality assurance measures record linkage techniques and duplicate resolutions, as well as joint definition of processes and workflows, communication principles including autonomous implementations, tests and the rollout of extensions for tools and workflows.

In January 2018 the Datenschutzkonferenz (DSK) published a short paper in which the German data protection authorities give important remarks for the future interpretation of the GDPR concerning data processing.[82] In March 2018 DSK published another short paper on joint controllers.[83] The two short papers must be read together as they complement each other. Although the short papers of the DSK are subject to reservation, they currently provide relevant guidance. The DSK sees the **decisive aspects in the definition of the purposes**, while the decision on the technical and organisational aspects of the processing may partly be delegated to the processor. This means, that to a certain extent, a processors scope for making decisions with regard to the means of the processing within a framework set by the controller does not per se exclude the classification as data processing.[84]

The data protection authorities have stated that the criteria for distinguishing between controller and processor, as applied under the old law, are no longer viable. Nevertheless they formulate comparable parameters, according to which it is a central criterion that the processor acts only and strictly instruction-bound.

> *"According to Art. 29 GDPR the service provider which is active due to an order is instruction-bound. He therefore does not carry out the processing for the controller as a third party in the sense of Art. 4 No. 10 GDPR. Rather, there is an "internal relationship" between the controller placing the order and his processor. Processing by the processor is therefore generally regarded as belonging to the controller."*[85]

This results in one of the main differences between data processing and joint controllership: the data processor is, so to speak, part of the controller. As a rule, the processor is allowed to do everything that the controller is allowed to do. Data transfers between controller and processor are allowed because they

81 Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 4 Nr. 7 Rn. 20, Fn. 34.
82 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018.
83 DSK, Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, Stand 19.03.2019.
84 DSK, Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, Stand 19.03.2019, p. 2.
85 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 1.

are treated like internal transfers. The controller is not a third party within the meaning of Article 4 No. 10 GDPR.

In contrast, there is no similar privilege between joint controllers. The entire cooperation, including the data transfers between the parties, would therefore have to be covered by a consent or legal basis. In the case of a declaration of consent, this would also have to refer to all controllers.[86]

It must therefore be examined on a case-by-case basis who determines the purposes and means. In difficult cases, the focus must be on who determines the purposes and whether one party may only process data strictly instruction-bound.

Since the TTP of UMG is legally a part of UMG, it should be noted that there can be no data processing relationships or joint controllerships between the TTP and the UMG as they are one entity. If, on the other hand, the TTP of the UMG acts for other bodies such as the DZHK, an assessment will be necessary. Since a TTP can take on different tasks and each task must be evaluated to determine whether it is being handled by joint controllers or a data processor, this can result in different classifications in different projects but also within a single project. If a TTP should become active in different roles within a single project, all roles could also be covered by a single contract. The GDPR does require contractual regulations, but not separate contract documents.

> *In which cases is it possible to act as joint controllers instead of working on the bases of a contract on data processing? (This would be much more suitable for scientific cooperation than data processing according to Article 28 GDPR.)*

As stated before, the cooperating parties cannot freely agree on their roles by defining them in a contract. The actual modalities of cooperation are decisive.

The DSK has listed examples in which joint controllership is to be assumed in Annex C of the abovementioned short paper on data processing.[87] Special reference is made to clinical trials for medicinal products. A joint controllership according to the DSK would exist if several participants (e.g. sponsors, study sites and physicians) each make decisions on processing in certain areas. The tasks of a TTP are not explicitly mentioned in the short paper. Typically, a TTP will make decisions on its own to a lesser extent than the DSK had assumed.

If a TTP only carries out pseudonymisations of IDAT which are provided for this purpose in an individual case and only specifies the measures necessary for this (with a certain decision-making power), this will presumably be understood as data processing according to Article 28 GDPR.

86 DSK, Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, Stand 19.03.2019, p. 1.
87 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 4, 5.

Should, on the other hand, the TTP collect personal data in addition to a specific research project of another controller also, e.g. as a register or repository, so that these data can be used later also by other controllers, this may qualify as a joint controllership for the platform thus created.

According to which argumentation criteria can joint controller processing be used and what are its consequences (in comparison to data processing)?

Joint controller processing has some minor advantages for the bodies involved, as some of the duties according to GDPR can be delegated between the joint controllers and both controllers are not instruction-bound.

However, there are also disadvantages that may not be counterbalanced by the advantages:

Firstly, as explained above, the privilege concerning transmission and further processing between joint controllers without a separate legal basis is no longer granted, which would, however, apply to data processing under Article 28 GDPR.

Secondly, all joint controllers are jointly liable for infringements of the GDPR and the damages that may arise as a result. This applies in the relation to the data subject independently of the contract clauses, which the parties can agree on in a contract according to Article 26 GDPR. In the internal relationship between the contracting parties (joint controllers) certainly clauses can be drafted in order to compensate such duties. Nevertheless the liability risk increases. There will especially include the risk that another joint controller may be insolvent and damages will have to be borne by the rest of the joint controllers alone.

Additionally, joint controlling must be reflected in the declarations of consent as the consent would have to cover the processing of all joint controllers.[88] Both the data processing and the joint control must be considered with the information duties under Article 13, 14 GDPR.

The DSK assumes that a joint control can increase the risk for the rights and freedoms of the data subjects and therefore a data protection impact assessment is more likely to be necessary.[89]

Contracts must be closed both in the case of data processing according to Article 28 GDPR as well as in the case the joint controllership according to Article 26 GDPR. The absence of such a contract is considered an infringement of the GDPR and can lead to administrative fines. In joint controllership, the law requires that the essence of the agreement shall be made available to the data subject in an applicable way (Article 26 para. 2 S. 2 GDPR).

88 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 1.
89 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 4.

Are existing contracts to be adapted and amended after the GDPR came into effect, e.g. because they regulate the transfer of functions ("Funktionsübertragung") and the waiver of data processing (under former data protection law)?

It cannot be said in general terms that all data protection related contracts, which came into force before the GDPR, can be continued without examination and without change. The DSK stated that however contracts concerning data processing can stay in force without amendment if they already fulfil the requirements of the GDPR.[90] It should therefore be assessed whether the requirements contained in Article 28 GDPR are met by the specifics of a project.

The German characteristic "transfer of functions" ("Funktionsübertragung") has only very limited significance under the GDPR. Since the old German data protection law only distinguished between a controller and a data processor and did not cover the concept of joint controllers, it could be determined in the case of the transfer of functions to other bodies that such a body would qualify not as a data processor but a separate controller. Under the GDPR, however, it cannot be determined without further ado on the basis of the idea of a transfer of functions whether there is a separate controller or a joint controller.

A separate controllership is a reasonable option if the controller transfers data to another controller without determining the purpose or means, to a situation in which the separate controller is in a position to process the data within determined limits at his own discretion. Any cooperation that is determined by means and purpose at the discretion of the initial controller are determined to be processing on behalf of the controller or joint controllership.

Neither the old nor the new law allowed cooperating bodies to agree with each other on whether there was a data processing. Therefore, no effective waiver could exist in a contract. Contracts that included a transfer of functions or an agreement that included a waiver for data processing should be checked very thoroughly.

Summarizing the above it can be concluded that data processing on behalf of the controller as well as joint controllership require a contractual basis. Both relationships can be part of a corporation contracted which would not be unusual. It should be assessed on a case-by-case basis which procedure would be best and in which cases neither would apply if the data processing is just a scientific task that would not be part of either category. Any project can encompass tasks that either processing, controllership or scientific work which are neither processing nor controllership. The corporation contract can assign these tasks to any of these categories.

90 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 2.

Appendix

List of Questions

Transparency

Art. 5a) GDPR sets standards for the transparency of the processes involved in data processing. In reference to this Article:

- Which technical and organisational measures must be implemented in order to achieve the required level of transparency?
- Is a combination of manual and automatic processes advisable/permissible here (cf. examples GMDS guidelines)?
- Can the necessary obligation to prove transparency be realised alternatively by a suitable passage in the data protection concept? (e.g. "within the TTP the TTP employee may carry out the processing according to consent")

Auditing

To document cross-system processes, audit logs are created by different systems.

- To what extent may these logs contain general information (for example, nurse A created patient with pseudonym A1B2C3 in system B and stored a consent with date xx/xx/2018)?
- May these logs contain personal identifying data such as "Max Müller, date of birth: 21/05/2001)?
- May server logs in selected higher log levels for the development and debug process ("service case") such as DEBUG or TRACE contain IDAT for troubleshooting (i.e., log level must be set explicitly, not the normal ones)?
- Which data can be retained in the event of a withdrawal of a declaration of consent? What must and can be "masked" practically? Where is the line between data protection and the need for IT and information security?

The right to be forgotten

Art. 17 GDPR guarantees a data subject's right to be forgotten.

If pseudonyms are generated and assigned to a unique personal identifier (mapping) and this assignment of a PSN-Value relationship is deleted (virtual anonymisation), no more conclusions about the identity of a person can be made within the TTP.

- Does this procedure correctly implement the right to be forgotten?

Erasure of Personal Data in backups

Data are regularly part of incremental or complete backups or dumps, which are written on tape as a series that partly rotates with a long cycle (years). Backups are generally encrypted. In the case of withdrawals or deletion requests, how do we deal with the fact that it is almost impossible to clean all series and databases in backups? Please develop and suggest a data protection compliant procedure model for this.

Information Duty

According to Art. 13 GDPR, a person must be informed comprehensively about the data collected. Must this be done immediately or is it permissible to wait for a request and provide information within a reasonable period of time (e.g. 4 weeks)?

Informed Consent

Information provided by a physician or study nurse (what turns consent into informed consent)

- Who can or must conduct an informative talk with the patient in order to guarantee an informed consent? Can this be done by trained personnel (study nurse, receptionist etc.)? Which other conditions must be observed?

In an international context, a uniform, quality-controlled consent form in English can be the means to elect to consent.

- Is a (supplementary) country-specific consent advisable here?
- Is the TTP obliged to validate the linguistic correctness e.g. of Lithuanian, Polish or Estonian consents?
- Does the TTP have to be able to assure the quality of these consents and guarantee their correctness? Only in this case, the TTP may not be able to validate/check the consents and handle or correct errors.

For logistical reasons, the original paper consent remains at the respective location and only a scan of the document is transmitted in encrypted form to the TTP consent management system.

- Is this procedure also legally secure from the point of view of the GDPR?

According to the GDPR, consent can be given by electronic means. Does this officially allow the sole use of digital signatures? (i.e. no paper-based consensus is obtained, the signature is recorded and stored directly electronically). Are both of the following options of the electronic signature permitted?

- Option 1: Capture via tablet PC and only the signature in reproducible form.
- Option 2: Capture via SignPad and signature in reproducible form including biometric information. The complete signature data record is stored in the database.

How is the use of signature devices, e.g. from sign-o-tec (store biometric data, not only the optical course of the signature) to be seen in relation to the two variants permitted under the German Civil Code (written form requirement or qualified electronic signature)? Under which conditions can Signpads be used hospital-wide for digital collection of the signature and the treatment contract?

Validity of consent forms, validity differentiation, and deficiency in quality

- When is a consent valid: a) only with signature of the participant or b) only with signature of the participant and signature of the informing person?
- Are dates on the consent mandatory?
- Is an invalid consent merely a quality defect or must it be a mandatory prerequisite for data collection?
- What differences must be taken into account in this regard for AMG or MPG studies compared to "normal" studies within the framework of the professional code of conduct?
- Are there different validity criteria for consents for the collection and publication/transfer of data?

Standard Operating Procedure (SOP)

According to Art. 6–11 GDPR, all data processing operations should be able to be agreed to separately. In addition, the data processor must comply with an accountability obligation (which data have been agreed to) and a process for the withdrawal procedures must be implemented. Within the framework of the Trusted Third Party, the consent management gICS and Standard Operating Procedures are used for these purposes. Are the requirements of the GDPR sufficiently implemented in this way?

Ethics Committee Vote

- Is the existence of an ethics vote a mandatory prerequisite for the activation of a site and the start of data collection at this site?
- In what form and to what extent can or must the data processor (TTP) prove the existence of the ethics vote and possibly other legal bases as a prerequisite? Who bears which responsibility?
- What is the legal (not: contractual) minimum standard before the data processor can perform his services in conformity with the law, what

requirements must be met before the TTP "activates" a study centre, a study or a project?
- In EU projects: To what extent is the TTP obliged to check the correctness of the ethics vote in the national language (e.g. Greek), or is work on a "basis of trust" sufficient?

Quality assurance in the Trusted Third Party

The declaration of consent is considered a central legal document in order to legitimise the processing of study participant data. Therefore, quality assurance measures are carried out on these documents and data in the TTP. As mentioned above, the TTP sends monthly quality reports with specific deficiencies on declarations of consent that require revision. These can be misspelled names, missing signatures or insufficiently marked consents.

The Trusted Third Party of the DZHK currently exclusively supervises multicentre studies (more than 70 affiliated centres). The reports are generated on the basis of the study and the centre and are currently transmitted via encrypted communication to a contact person of the student assistant and must be distributed from there.

- Is the above procedure sufficient to ensure a centrally controlled verification of the consent status for the release of data and samples?
- What further measures might need to be taken?

Authorisation of Study Leaders

To date, the central study leaders have had the right to access and at least view all medical, laboratory and image data of a study participant in other centres.

- Do these persons also have the right to view all identifying data of the study participants?
- What about multicentre studies? Do the German Medicines Act (Arzneimittelgesetz—AMG) and the Medical Devices Act (Medizinproduktegesetz—MPG) studies contain any requirements in this respect?
- How is the viewing of such data regulated in other EU Member States?
- What measures might need to be taken or adhered to with regard to such access?

Dealing with different consent versions

As part of the study preparations, the declaration of consent for a new study is given to an ethics committee. This committee prepares an ethics vote for the submitted documents in the current version. The TTP assumes that in a study with a valid ethics vote, study participants may only consent to the respective declaration of consent. If the content of a consent changes, it must

be voted on again and a new version of the consent must be created accordingly.

If a multicentre study decides to change the content of a consent form, it must in most cases be submitted to all competent local ethics committees. It makes operational sense that uniform versions are always used across all centres. In the case of a version change, the trustee assumes that recruitment must continue with the consent form voted on (e.g. 1.0). Even if the study centre (e.g. Berlin) already has a vote for a newer version (e.g. 1.5), all centres must (according to the previous definition) recruit with the existing and universally voted version (e.g. 1.0) until all centres have a uniformly voted version. What is your legal assessment of this situation? Are study centres allowed to recruit a study with different consent versions at all, or do they have to be uniform throughout the study?

Dealing with deceased study participants

In a few cases, the trustee is informed that study participants have died during or after the study. The TTP assumes that the death of a study participant does not result in any changes and that no additional measures need to be taken. Any withdrawals by relatives of the deceased are implemented in the same way as during the participant's lifetime. Is this correct and legally permissible?

Studies within the European Union

Several multicentre studies in the DZHK are taking place not only in Germany but at international locations. Data is also intended to be collected in non-German centres with the aid of previously established infrastructure. This means that the TTP is also utilised as the central facility for managing individuals and consent forms. For example, a Polish centre has barred the input of data and transmission of the consent forms to the TTP because this violates national data privacy and protection law.

- What national legislation in EU Member States presents an obstacle to such processing?
- What kind of measures need to be taken so that the TTP can fully complete the data processing (= processing as performed in Germany) despite a national restriction?
- What differentiations between registers and AMG/MPG studies are stipulated in the individual Member States?

Data transfer within the EU

As a rule, data transfer within the EU is not restricted.

- Can the transmission of IDAT to a central controller be restricted by local regulations above and beyond the GDPR and is it restricted in DZHK countries, such as (for example) in Poland?
- Are there particular legal situations in Poland in which IDAT is not permitted to be transmitted to Germany and processed there (despite consent having been obtained)?
- How substantial is such a "refusal" by the ethics committee (in this example, the Polish committee) that "determines" that IDAT is not "permitted" to go to a central TTP; is this substantial and is the DZHK TTP required to accept it?

Withdrawal of a declaration of consent/study exclusions

Within the scope of the withdrawal process, the data of a participant will be anonymised. The medical data is also locked for further data transfer and can normally not be processed further.

- How should this regulation be viewed in connection with AMG/MPG studies? Can data still be supplemented or edited after the withdrawal?

Paper-based consents include the source-specific primary pseudonym of the participant.

- Should this pseudonym be blacked out/cut out in the consent?

Withdrawal of a patient means the blocking and anonymisation of the data. The data will only be deleted upon explicit request.

- Is this procedure permissible?

When implementing a withdrawal, biomaterials must be destroyed and proof of destruction (technical notification, completed paper form, scan) must be provided.

- Is a simple database entry in the Audit Trail sufficient or do we have to have an original paper for legal reasons and keep it in a written form according to the German Civil Code (BGB)?
- What exactly is TTP responsible for? Control of destruction or only request for destruction and obtaining confirmation of success?

Consents (before 25/05/2018)

The TTP administers consents of patients who were collected before 25/05/2018. Individual consents use a passage on the use and transfer of data (including

"third countries with lower data protection levels"). A large number of patients have agreed to this passage.

- Are these still permissible under Chapter 5 of the GDPR or must new consent be obtained?
- How does this regulation behave in particular with regard to cooperations with the USA?

Consent (after 25/05/2018)

Does the GDPR permit the following consent clause? What content adjustment would have to be made if necessary?

"Pseudonymised data and biomaterials may be transferred to countries for which the European Commission has not determined an adequate level of data protection".

Storage limitation

Clinical research projects funded by the DZHK take place in the public interest and the measures required by Art. 89 GDPR to protect data (separation of powers, data minimisation, pseudonymisation, anonymisation) are implemented. Storage for an indefinite period is essential for the collection of data and biomaterials to be used beyond the study period.

- Are the storage and use of personal data and research data still permissible for an indefinite period of time after the data subject has been informed about this and has consented accordingly?
- How is the retention period of consent and research data defined by the GDPR?
- Is it advisable to secure the storage period of the data and the consents by the consent itself?

Purpose limitation

At present, the study consent also allows the use and transfer of personal data for biomedical research projects. The consent is obtained without the possibility to exclude this purpose.

According to Art. 5b) GDPR "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes.

Can further processing for purposes other than the study purpose (but nevertheless within the framework of research) be carried out in accordance with consent?

End of a project

At the end of project funding (BMBF, DFG), TTP and IDAT remain in the "estate".

- What must the relinquishing office ensure before IDAT is handed over?
- What must the receiving institution prove before the TTP transfers and deletes its data?
- What is normal/usual/allowed at the end of a project, if the erasure of the data is not forced by consent/study protocol … for example in clinical epidemiological projects? Can the TTP switch off the services but continue to store the data without an ongoing project? Under what conditions?
- How long after the end of the project must the storage of a) consents and b) research data be ensured, unless otherwise specified?
- Is it possible to transfer MDAT and/or IDAT to third parties after the end of the project?
- Under what conditions is the transfer of TTP data (Identifying Data [PII], pseudonyms + mappings, consents and withdrawals) to third parties permissible after the end of the project?
- Under what conditions is the transfer of research data to third parties permitted after the end of the project?
- Who is responsible for checking the suitability of the third party as data trustee/processor?

Possession and ownership of data

- Who is the data possessor, the data owner and the data processor in the context of the data processing described?
- How do these terms exactly differentiate themselves from each other?
- Who is the data possessor and data owner after the project has ended?

Data Protection Management System

Art. 5 and 24 GDPR demand the establishment of a data protection management system (DPMS).

- Who is responsible for this establishment of a DPMS? (Designated data protection officer?)
- The specifics of the Data Protection Management System are not comprehensively described in the GDPR. Can the drafting and review of a data protection concept or a legal opinion be regarded here as the implementation of a Data Protection Management System?

Privacy by Design

Art. 25 GDPR demands "Privacy by Design". The trustee approach includes (cf. [Bialke, et al. 2015]):

- informational separation of powers
- separation of IDAT and MDAT
- use of ID management according to the Master Patient Index concept for record linkage
- use of pseudonym management
- digital consent management and modular Informed Consent approach
- workflow-controlled TTP dispatcher approach for overarching complex TTP workflows
- Is the trustee approach presented suitable for implementing the goals of Privacy by Design?

Use of eGK number or KV number

- Are the electronic health card (eGK) and health insurance number (KVNR) particularly items worthy of protection in terms of data protection?
- Under what conditions may the TTP collect/process these data, is an explicit consent (consent policy) necessary for this or can these items be processed as IDATs?
- Under what conditions may TTP use this data for matching (determination of a person's identity)? (ID with wide scope for merging data)

Technical and Organisational Measures (TOM)

- What TOMs are compulsory for the party processing the data (UMG)? Please provide specific examples, e.g., server certificates, TLS 1.2, multi-tenant architecture, measures relating to space and personnel, network segmenting, IP filters, …
- What TOMs are compulsory for the party entering the data (e.g., hospitals in Germany, Poland, Lithuania, Estonia)? Please provide specific examples, e.g. browser specifications, client certificates, TLS 1.2, providing their own pseudonyms, …

Data usage by industrial partners

- Which legal framework must apply if research data already covered by consent are to be used for secondary research and/or by industrial partners (e.g. for quality assurance of implants)?

Necessity of documents

The GDPR requires the creation and maintenance of extensive documents and directories.

- Which documents are legally mandatory according to the GDPR (e.g. data protection concept, description of procedure, list of procedures)?
- Is it legally necessary to carry out a data protection impact assessment? If so, please advise us on the (document) form, scope and level of detail of this data protection impact assessment.
- Which documents are mandatory for DFG- or BMBF-funded research projects and what can be stored if necessary?

Responsible supervisory authority

- Data subjects have the right to lodge a complaint with the responsible supervisory authority. This should be specified precisely in the consent. In the case of an EU-wide project: which authority is the responsible supervisory authority in this case?

Release from obligation to secrecy

- What happens if the current consent form does not provide for an explicit release from the duty of confidentiality according to § 203 StGB?
- Which test criteria can be used to determine algorithmically whether a release from the duty of confidentiality is required in a project?

Necessity of a contract on data processing

- When does the GDPR require the conclusion of a contract on data processing?
- In which cases is it possible to act as joint controllers instead of working on the bases of a contract on data processing? (This would be much more suitable for scientific cooperation than data processing according to Article 28 GDPR.)
- According to which argumentation criteria can joint controller processing be used and what are its consequences (in comparison to data processing)?
- Are existing contracts to be adapted and amended after the GDPR came into effect, e.g. because they regulate the transfer of functions ("Funktionsübertragung") and the waiver of data processing (under former data protection law)?

Keywords Glossary

AMG	Arzneimittelgesetz	Medicinal Products Act
BDSG	Bundesdatenschutzgesetz	Federal Data Protection Act
BGB	Bürgerliches Gesetzbuch	German Civil Code
BGH	Bundesgerichtshof	Federal High Court
BSG	Bundessozialgericht	Federal Social Court
ECJ	Europäischer Gerichtshof	European Court of Justice
GG	Grundgesetz	Basic Law for the Federal Republic of Germany
MPG	Medizinproduktegesetz	Medical Devices Act
SGB I	Sozialgesetzbuch (SGB) Erstes Buch (I)—Allgemeiner Teil	German Social Code—Book I
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V)—Gesetzliche Krankenversicherung	German Social Code—Book V
SGB X	Sozialgesetzbuch (SGB) Zehntes Buch (X)—Sozialverwaltungsverfahren und Sozialdatenschutz	German Social Code—Book X
SOP	Standard Operating Procedure	Standard Operating Procedure
TOM	Technische und organisatorische Maßnahmen	Technical and organisational measures
TTP	Unabhängige Treuhandstelle der Universitätsmedizin Greifswald, K.d.ö.R.	Independent Trusted Third Party of the University Medicine Greifswald (public body)
UMG	Universitätsmedizin Greifswald	University Medicine Greifswald
StGB	Strafgesetzbuch	German Criminal Code

Zur Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.

In der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. arbeiten Netzwerke und vernetzt arbeitende Einrichtungen gemeinsam daran, die Fragestellungen und Herausforderungen von medizinischer Forschung an verteilten Standorten zu lösen, ihre Erfahrungen zu bündeln und damit zu mehr Transparenz und Effizienz im Gesundheitswesen beizutragen. Durch den Community-Ansatz erfahren die Ergebnisse der TMF eine breite inhaltliche Abstimmung in der medizinischen und medizininformatisch-biometrischen Fachwelt. Mit ihrer Schriftenreihe macht die TMF die Lösungen einer breiteren Leserschaft zugänglich.

Bisher in der Schriftenreihe erschienen:

Band 1:
Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin
von Carl-Michael Reng | Peter Debold
Christof Specker | Klaus Pommerening
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 2:
Biomaterialbanken – Rechtliche Rahmenbedingungen
von Jürgen Simon | Rainer Paslack | Jürgen Robienski
Jürgen W. Goebel | Michael Krawczak
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 3:
Checkliste und Leitfaden zur Patienteneinwilligung Grundlagen und Anleitung für die klinische Forschung
von Urs Harnischmacher | Peter Ihle | Bettina Berger
Jürgen Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 4:
Datenqualität in der medizinischen Forschung
von Michael Nonnemacher | Dorothea Weiland
Jürgen Stausberg
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2007

Band 4, 2. Auflage:
Datenqualität in der medizinischen Forschung
von Michael Nonnemacher | Daniel Nasseh | Jürgen Stausberg
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2014

Band 5:
Biomaterialbanken – Checkliste zur Qualitätssicherung
von Michael Kiehntopf | Klas Böer
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2008

Band 7:
Verwertungsrechte in der vernetzten medizinischen Forschung
von Jürgen W. Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2009

Band 8:
Regulatorische Anforderungen an Medizinprodukte
von Kurt Becker | Sandra Börger | Horst Frankenberger
Dagmar Lühmann | Thomas Norgall
Christian Ohmann | Annika Ranke | Reinhard Vonthein
Andreas Ziegler | Andreas Zimolong
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2011

Band 9:
Qualitätsmanagement von Hochdurchsatz-Genotypisierungsdaten
von Michael Krawczak | Mathias Freudigmann (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2011

Band 10:
Einwilligungserklärung und Forschungsinformation zur Gewinnung tierischer Proben
von Jürgen W. Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2012

Band 11:
Leitfaden zum Datenschutz in medizinischen Forschungsprojekten
von Klaus Pommerening | Johannes Drepper
Krister Helbing | Thomas Ganslandt
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2014

Band 12:
Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen
von Uwe K. Schneider
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2015

Band 13:
Terminologien und Ordnungssysteme in der Medizin
von Otto Rienhoff | Sebastian C. Semler (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2015

Band 14:
Gesundheitsforschung kommunizieren, Stakeholder Engagement gestalten
von Wiebke Lesch | Antje Schütt (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2016

Band 16:
Big Data im deutschen Gesundheitswesen – Handlungsempfehlungen
von Sebastian C. Semler | Karoline Buckow (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2019

Band 17:
Sekundärnutzung von Sozial- und Gesundheitsdaten – Rechtliche Rahmenbedingungen
von C. Dierks | A. Roßnagel
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2019