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).

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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].

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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).

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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-

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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.

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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.

Auszug aus: Dierks et al., Data Privacy.
ISBN: 978-3-95466-592-1

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.