Biobanking **Edited by: M. Kiehntopf**

Johannes Drepper*

Data protection in biobanks from a practical point of view: what must be taken into account during set-up and operation?

https://doi.org/10.1515/labmed-2018-0112
Received August 7, 2018; accepted December 17, 2018; previously published online July 26, 2019

Abstract: The European General Data Protection Regulation (GDPR) incorporates many of the principles of data protection that were already in force in the past. Insofar the data protection requirements for German biobanks have not fundamentally changed since the GDPR became applicable in May 2018. In detail, however, new and relevant requirements have been added. Due to many derogation clauses that allow national deviations, federal and state laws must also be taken into account in Germany, depending on the legal form of the biobank or the supporting institution, which increases the complexity in individual cases. Research-oriented biobanks can still rely on informed, voluntary and explicit consent from patients or test persons. Other legal bases are also possible in certain cases. The information and transparency requirements have increased with the DSGVO, which has led to higher administrative costs. However, a major problem existed before and continues to exist in clarifying how biobanks deal with the right to know and the right not to know of their subjects, how this is explained in advance and which policy can be implemented in the long term, also in the context of targeted recruitment for later studies. The complexity of the regulatory framework and the resulting demands on biobanks make the development and implementation of standards unavoidable. In addition, it is recommended that such infrastructures be centralised, professionalised and equipped with the necessary resources.

Keywords: biobanks; data protection; data protection concept; General Data Protection Regulation; informed consent; right not to know; right to know.

***Correspondence: Johannes Drepper,** TMF e.V., Charlottenstr. 42, 10117 Berlin, Germany, E-Mail: johannes.drepper@tmf-ev.de

Overview of the legal framework

Data protection for German biobanks must always be viewed from two different directions: On the one hand, samples usually contain extensive genetic information that is fundamentally personal or at least offers considerable potential for re-identification; on the other hand, the samples stored in biobanks usually unfold their particular value for research only when they are linked with as extensive, phenotypic data as possible, so their storage in accordance with data protection regulations must also be guaranteed.

Where data that can be traced to a person directly or indirectly are processed, data protection law must always be applied, although it is distributed over a wide range of different laws at different levels and depending on the framework conditions. This is not exactly conducive to obtaining a uniform overview.

First of all, one must mention the European General Data Protection Regulation (GDPR), which has been directly applicable in the Member States of the European Union (EU) or the European Economic Area (EEA) since 25 May 2018. This has given the national legislator concrete tasks to regulate certain areas of data protection independently, such as the responsibility of supervisory authorities. But the GDPR also contains in some places so-called derogation clauses, which give the Member States or the EU the possibility to design certain areas of data protection differently. Accordingly, the German legislature has already passed a new Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), which was applied simultaneously with the GDPR and refers specifically to the regulatory obligations and scope under the GDPR.

The scope of application of the BDSG extends to federal public institutions and privately supported institutions. However, many biobanks are now set up in hospitals, for which, being public institutions of the respective federal states, the state data protection law initially applies. This is particularly true of the large biobanks at university clinics that are partly funded by

the Federal Ministry of Education and Research (BMBF). At the same time, some state data protection laws refer in turn to the regulations of the BDSG (e.g. Section 2(5) of the Data Protection Act for the State of Mecklenburg-Western Pomerania) in connection with public institutions that compete with private institutions. However, as hospitals – irrespective of whether they are public or private institutions – are in competition for treatment conditions and possibly also for research funds, such a reference to the BDSG must be followed and parts of the BDSG applied ([1], p. 126). After a first adjustment to the BDSG, state data protection laws have also been overhauled. It still remains to be seen if this will be followed by further adjustments. For the BDSG, there is already another draft amendment being circulated, but it is to address only specific details.

For the biobanks at hospitals that are part of general care or are included in the respective state hospital plan, the respective state hospital law may also apply. This is at least the case when the biobank is also involved in the care process or is used in the care context. In these cases, due to the backstop nature of data protection laws, some data protection regulations contained in the state hospital laws must be considered first and foremost. However, the state hospital laws have not yet been fully adapted to the GDPR. In this context, it is still unclear whether already existent laws continue to apply with reference to the very far-reaching derogation clause in Art. 9(4) GDPR.

In addition to the data protection regulations in the various laws as a second independent barrier against reuse, medical secrecy under Section 203 of German Criminal Code (Strafgesetzbuch, StGB) has to be considered, if the data or samples originate from a treatment relationship and are to be shared with researchers not directly involved in the treatment context.

Furthermore, doctors or physician-led projects in the field of biobanking are subject to the professional regulations of the states, which define additional framework conditions for research, such as consultation with an ethics committee as required by Section 15 of the Model Professional Code of the German Federal Medical Association, if a project involves samples or data that can be traced to a particular person. Important ethical and professional requirements can also be found in the internationally agreed rules of the World Medical Association, such as the well-known Declaration of Helsinki [2] or the more specific Declaration of Taipei on health databases and biobanks [3].

Schneider has examined the legal framework for the reuse of clinical data (and samples) prior to the adaptation of national laws to the GDPR and has come to the problematic conclusion that the differences in the regulations in the individual states also have very practical consequences, which can actually cause a serious problem for projects. Accordingly, even the clarification of the applicable legal framework for a specific hospital can be surprisingly complex [1].

Even though the current situation of the state-specific regulations following their adaptation to the GDPR has not been studied yet in such detailed manner as that of Schneider, a first look already reveals that our federal regulatory jungle shows hardly any trace of the harmonisation intended by the European legislature. However, the harmonisation of data protection law with the GDPR was addressed only half-heartedly. As Roßnagel notes: “In light of the abstractness and undercomplexity of its [GDPR] regulations, it was necessary to grant Member States 70 derogation clauses for diverging legal regulations” ([4], p. 478). Accordingly, Roßnagel does not expect a standardisation of the current data protection law, but sees a co-regulation by legislators in the Union and the Member States established through the GDPR ([4], p. 481).

Legal foundation

For the collection, storage and processing of samples and associated health data, a data-protection permission is necessary due to the data – and, as a rule, also the samples – can be traced to specific individuals. This may involve a legal basis for processing, or also an informed consent that meets the data protection requirements.

When collecting samples, in addition to the data protection regulations, further framework conditions must be taken into account, as this situation may also affect the right to physical integrity, for example. A distinction must be made here as to whether the samples were taken entirely in the context and for the purpose of care and only unexpectedly unused residual sample materials are available for research, or whether additional material is sampled as part of a medical procedure, or whether an entirely separate medical procedure is required to collect material for research. Due to this paper’s focus on the data protection framework, these different case constellations and their legal assessment beyond data protection will not be discussed further. The literature provides good overviews on this subject [5, 6].

Consent

In order to obtain a data-protection permission for the processing of samples and contained or assigned data,

the affected person's consent is obtained in most cases. A model consent for biobanks was developed by the working group of medical ethics committees (AK EK) and published in 2013 for the first time in its agreed form. The current and revised version dates from 2018 [7]. This model consent also deals with and regulates the special case of consenting to a very broad use of samples. This includes, for example, uses independent of a specific disease area. So far, the conformity of such a "broad consent" with data protection law has been viewed as controversial [8]. At least, the European legislator has for the first time given expression in the GDPR to the problem that future uses can often not be defined in narrow and specific terms. Even if there is no uniform interpretation yet of the wording "certain areas of scientific research" to which one can consent, contained in Recital 33 of the GDPR, and of what precisely it entails, including how narrowly or broadly the purposes of use must or can be defined, it cannot be denied that the legislator has created additional scope for research where the delimitation of purpose is concerned.

Another important innovation of the consent regulations under the GDPR is the waiving of the written form requirement. Recital 32 of the GDPR provides that the consent can also be expressed by ticking a box when visiting an internet website. It is important to note, however, that the controller under Art. 7(1) GDPR must be able to demonstrate that the data subject has consented to the processing of his or her data.

However, the European legislator has left national legislators with plenty of scope for independent and even tighter regulations, especially with regard to dealing with health and other particularly sensitive data. This even includes the exclusion of consent in special cases [cf. Art. 9(2)(a)].

Accordingly, it must be clarified for each case of application whether the EU GDPR is directly applicable or whether the national legislator has exercised its own regulatory authority. In Germany, the national regulatory authority in the field of public institutions also affects the individual states, so provisions on consent contained in state data protection laws or state hospital laws may have to be observed as well. If these are narrower than the provisions of the GDPR, then this is to be construed as a legitimate use of the derogation clauses of the GDPR for national legislators and must be taken into account accordingly. There is still no overview of more specific wording on consent in state law, as Schneider has provided for the situation before adaptation to the GDPR [1], for the current legal situation. Nevertheless, the national legislator at the federal level has not included any specific wording on consent to the use of health data in the new Federal Data Protection Act (BDSG), which means that the EU regulation applies directly to applications in its scope.

Consent to the use of data and samples from a treatment context should always also meet the requirements for a release from confidentiality. Even if a data-protection consent, if it refers clearly to the further use of samples and data from the treatment context, can be understood as an implicit release from confidentiality, an explicit reference to the release from medical confidentiality, insofar as the data are derived from the treatment context, ought to be included in the declaration of consent.

But in addition to the data protection law that is the focus of this paper, which goes back to the general personality right of the sample donor, the ownership right is also to be considered in the further use of biomaterials. This is initially due to the donor, and it is disputed whether a donor, with his or her consent to the use of the sample for research, also implicitly gives up his or her ownership and/or transfers it to the biobank (cf. [5]). However, today it is generally recommended to include an explicit reference to transfer of ownership in consent declarations [7, 9]. This applies in particular if subsequently an economic utilisation of the samples is planned, for example. Despite transfer of ownership, however, the donor retains personal rights in respect of the sample. This may also mean that after a sale of the sample the buyer will be forced to destroy the sample classified as personal if the donor withdraws his or her consent. For merchants, this is certainly a hard-to-understand scenario, which, however, appears to be quite simple and comprehensible for lawyers based on the interaction of two different legal spheres.

One question that is certainly asked frequently concerns the handling of consents already obtained prior to the applicability of the GDPR, if the data continue to be processed – that is, in accordance with the GDPR. In this context, it is worth taking a look at the recommendation of the EU's Article 29 Working Party regarding consent under the GDPR [10]. According to this recommendation, a new consent does not have to be obtained in every single case.

What is important is that the old consent, too, must have met the basic requirements of the GDPR. This includes in particular that the consent was given voluntarily and explicitly (as opposed to an "opt-out"). Furthermore, the consent must have indicated the specific purposes and provided sufficient information on options to revoke consent. Even if the extended information obligations under Art. 12 and 13 GDPR (a more detailed description follows in the section on patient rights) have not yet been implemented, this does not mean that a new consent has to be obtained in every single case.

Such information can also be provided, for example, by posting generally available information on an internet website.

Research clauses

But there are also application cases or research projects that are difficult to carry out on the basis of consent, be it because this would lead to an expected significant selection bias or because the associated effort would in any case prevent the research project. Also, obtaining consent may be impossible from the outset, as is the case, for example, with some old-sample collections for which there are no longer any assignment lists with patient identifiers. In such cases, it is necessary to examine whether there is a possible legal basis in the applicable legal framework for the processing of samples and related data. Such regulations can be found, for example, in the research clauses in the BDSG and possibly in some state hospital laws. In individual cases, these research clauses permit the execution of research projects on the basis of personal data, if the interest in the implementation of the project considerably outweighs the individual interest of the data subjects in the exclusion of their data from the processing and the project would not be feasible otherwise as it relies on the data (cf. Section 27(1) BDSG). Individual state laws may provide for additional conditions, such as regulatory approval, which means that the applicable law must always be identified and verified. For biobanks, it should also be noted that such data protection legislation concerns only the processing of personal data and does not contain any provisions about the legitimacy of the collection of additional sample material for research. The samples can therefore only be used if residual material is available anyway and its use in the research context does not hinder or prevent any subsequent necessary diagnostics.

As explained earlier in this paper, samples and data from the treatment context are always also subject not only to the legal data protection framework but also to the additional and independent medical confidentiality obligation. The corresponding professional and criminal regulations take precedence over data protection laws and are not suspended or restricted by them. While data protection law governs in particular the change of purpose for the re-use of samples and data from the treatment context, medical confidentiality concerns solely the disclosure of personal data. A purpose-changing secondary use of treatment data is therefore compatible with confidentiality, provided that no personal data are given to persons who are not involved in the treatment context of the affected patients. In other words, the research clauses in data protection law may permit the change of purpose, but not the disclosure of the data to persons not involved in the treatment. Accordingly, the aforementioned research clauses as permissive rules apply in most cases only to so-called internal research projects and cannot be used to legitimise the transfer of samples or data within the framework of cooperative research projects. Exceptions to this exist only if such permissive rules are found in state hospital laws and also explicitly regulate the transfer of data. Such regulations in state hospital law as a special standard are then also construed as authority of disclosure according to the secrecy obligation standardised in criminal law (Section 203 of the German Criminal Code) ([1], p. 50f).

For this reason, a distinction must be made between purely internal research projects and those that involve the disclosure of samples or data, and it must be examined on a case-by-case basis whether a suitable permissive rule can be found in the applicable law.

Another difference between medical confidentiality and data protection law concerns the use of data and samples from deceased patients. While medical confidentiality applies beyond death, the data protection law restricting the change of purpose generally no longer applies here (cf. Recital 27 GDPR). Further information on medical secrecy on the one hand and related disclosure authority on the other can be found in Schneider ([1], pp. 75ff).

Data processing by a processor

Biobanks may be engaged by other entities as processors or may themselves involve other entities, such as laboratories, as processors. From the point of view of data protection law, it is important that when considering such division of labour, the processor has no independent decision-making power over the processing of data and any samples. However, under the GDPR regulations on data processing by a processor (Article 28), the processor has greater responsibility and new obligations than was the case in the data processing regulations under the old BDSG in Germany. In this respect, at least some details in contracts for commissioned data processing must usually be changed and concluded anew. The old BDSG, in its data processing regulations on commissioned data processing, clearly privileged such integration: The processor was explicitly not a third party, so the data transfer could not be regarded as an independently justifiable data transfer. However, it is to be asked whether this privileging continues also under the GDPR. The Conference of Independent

Federal and State Data Protection Officers made the following clarification in a brief on data processing by a processor under the GDPR: "For the transfer of personal data to the processor and the processing by the processor, there is normally no need for any further legal basis within the meaning of Articles 6 to 10 of the GDPR other than that on which the controller himself bases the processing." ([11], p. 2, translation by the author).

Patient rights

A topic that is always controversial and not accessible to simple solutions is that of the information rights of patients or sample donors. It is undisputed that, in relation to the data collected, there are extensive information obligations on the part of the data controller. These are standardised in Article 13 of the EU Regulation and go far beyond previous regulations in their details. As such, existing forms, brochures and other information materials may need to be adapted here. The framework conditions for this and for further patient rights are regulated by Article 12 of the GDPR. Article 14 GDPR also sets out the information requirements if the personal data were not collected from the data subject. This may refer to data subsequently obtained from samples, for example.

According to Art. 13 GDPR, the contact details of a data protection officer must be communicated to the data subject at the time of the data collection in addition to the previously necessary information on the controller as well as on the purposes and legal bases of the processing as well as its duration. In addition, explicit reference must be made to the existence of a right to lodge a complaint with a supervisory authority. It is important to note that the GDPR here requires differentiated information: Name and contact details are required of the controller (this is generally a data controller, that is, a legal entity), while any data protection officers must provide only the contact details. As for one or several competent supervisory authorities (the GDPR does not reflect this possibility of differentiation, as the regulation of supervision is largely left to the member states), only the reference to the abstract right to lodge a complaint is required, that is, without indication of a name or contact details of the respective supervisory authority or authorities.

In principle, Article 13(1)(e) also requires information on (subsequent) recipients or categories of recipients of personal data and, where applicable, samples. In the context of a "broad consent", it is usual that not all subsequent users and recipients of the data are mentioned at the time of the collection.

The only solution is to narrow down the category of recipients as precisely as possible at the time of the collection and to inform the data subjects. Moreover, potential recipients also include institutions, companies or institutes involved in data processing by a processor. It is therefore also necessary to provide information on them, and possibly also as a well-described category of recipients, if one wishes to ensure some flexibility in the subsequent selection of processors.

In addition to the previously customary references to the right of revocation and thus, implicitly, the right to erasure as well as the rights in terms of access and rectification, today one must also explicitly reference the right to restriction (formerly called blocking) and the right to data portability.

The right to data portability according to Art. 20 GDPR is fundamentally new and should by no means be confused with the long established right of access. At its core, this is more about strengthening competition in data-based services than genuinely privacy-related issues. Data provided by data subjects must therefore be provided directly in an electronic, standardised and interoperable manner to data subject or, at his or her request, to other providers as well. With regard to social networks, in which users provide practically all data themselves, the intention of such a regulation is quite understandable. But for clinical data or even samples, a reasonable applicability is more than doubtful. Although electronic patient records may well help the transfer of clinical data in the patients' interest, they go far beyond the requirements of data portability. After all, the only requirement here is the provision of the data provided by the patient or test subject himself or herself. In the clinical context, for example, this could be specific medical history data. Even the diagnosis, certainly a very central and important data set of any clinical data collection, is not to be regarded as a data set provided by the patient himself or herself. Thus, a strange set of data would have to be provided in an electronically standardised format, but there is, or will be, no such format, especially for such a fragmented data set of little use. Unfortunately, the European legislator has provided only exceptions to the requirement of data portability in view of the high bar set in Article 23. These require a corresponding national regulation of exceptions, which in turn must be well founded. There are no such exemptions in the new BDSG. As a result, at present, it is only possible to point out the right to data portability in general patient information and then, when referring to a patient, one has to clarify on a case-by-case basis whether data has been provided and how it can be made available.

Even though the administrative costs associated with these information rights under the GDPR should not be

underestimated, these rights do create problems that are not always easy to solve in ethical terms and without conflict, which in particular have to do with the difficult question of what patients or test subjects actually want to know about the analysis results based on their samples and what they would, perhaps, rather not know about. There are risky pitfalls in giving a biobank a purposeful orientation and these pitfalls are difficult to circumvent.

Test subjects may have a legitimate interest in the results of medical research, especially if these are individual results of medical relevance. The possibility of the emergence of such results can be excluded ever more rarely, particularly when extensive data and sample collections are used. Against this background, test subjects should be informed in advance about possible test results, and an appropriate arrangement for sharing information should be agreed with them. However, this is where things become difficult, because for biobanks with a long-term horizon it is often not possible to clearly state what test results may be obtained at some future point in time. It should also be remembered that test subjects may not want to be notified of certain test results. This may apply, for example, to results from genetic tests or other findings of a predictive nature. This right to not knowing must also be taken into account in corresponding agreements [12, 13]. In this context, test subjects should also be informed that they may have to disclose test results known to them to insurance companies or employers, for example. On the other hand, results from genetic tests may also be relevant for relatives of the test subject, which means that their right to not knowing must also be taken into account [14]. Should a test subject insist on being informed about the results of genetic tests, then such a request cannot be denied because of his or her informational right of self-determination. However, he or she may then come into conflict himself or herself if he or she wants to tell relatives that relevant information from genetic testing exists, while having to respect their right to not knowing. Test subjects should therefore be alerted in advance to such a potential conflict situation. When determining a standard procedure, which can also be deviated from within the scope of graduated informed consent, it should be taken into account that many random findings from genetic or other tests with low actual relevance for the test subjects can at the same time also create considerable uncertainty. What is more, the effort of informing test subjects is not to be underestimated: counselling will have to be provided, and reverse pseudonymisation, including all complications involved, will have to be regulated. With regard to reverse pseudonymisation, it may be necessary to think of any necessary releases from confidentiality, or technical and organisational procedures must be implemented to ensure that only the attending physician receives the test result in a non-pseudonymised form. Against the background of the aforementioned efforts and the relevance of the communication of incidental findings that may often be insignificant, a research project may be set up in such a way that the subjects initially waive the right of notification with the declaration of consent. This can also be made a condition for participating in the research project [15].

However, it should be noted that test subjects can also revoke this agreement and will be entitled to their right to information at a later date. An irrevocable waiver of communication of test results cannot be agreed with test subjects. An agreed waiver regarding the communication of results may, however, in certain cases limit the subsequent recruitment of subjects. This may be the case, for example, when predominantly or exclusively patients are to be recruited for a prevention study who have certain risk factors and the agreed waiver implies that the subject is not to be informed of the existence of such a risk factor.

Furthermore, a patient's right to information may have to be differentiated from medically justified notification obligations on the part of researchers. These relate, for example, to important medical findings with immediate consequences for further treatment or diagnosis. In principle, it should be noted that all of the patients' information rights and the reporting obligations of the researchers refer only to data that has not been anonymised.

Data protection concept

If samples and data for medical research are to be stored for a longer period of time and, if necessary, used for less restricted purposes, more complex protection procedures as well as long-term and binding regulations of responsibility will have to be put in place. This is also the core of the self-regulatory approach for medical collaborative research in Germany initiated by the Technology, Methods, and Infrastructure for Networked Medical Research (TMF) as an umbrella organisation for networked medical research in Germany and coordinated with the supervisory authorities of the Conference of Independent Federal and State Data Protection Officers [16]. With regard to the pseudonymisation and, where appropriate, anonymisation procedures to be used to hedge against the risks, a distinction must be made between the treatment of samples and data. Even if many authors today still assume that samples can be made anonymous, it should

be borne in mind that the costs of re-identification based on the genetic information contained in a sample will continue to decline. Accordingly, at least in the foreseeable future there will hardly any disproportionate effort involved in re-identifying a sample. But that would be exactly the requirement for an anonymous sample. In this respect, one can only recommend pseudonymisation for current and future research projects where the long-term management of samples is concerned. This also has the advantage that donors are not unnecessarily hampered in the subsequent enforcement of their personal rights existing on the sample.

Anonymisation of the data associated with samples, however, can always be achieved, in particular if the data are well defined and structured, by means of appropriate coarsening and modification procedures. However, the costs involved and, in particular, the resulting limitations on the further scientific usability of the data processed in this way should not be underestimated [17].

As a rule, in addition to the described problems of anonymisation, there are also scientific and possibly ethical reasons in favour of pseudonymous data and sample management. For example, this may involve data and samples obtained at different times or in different contexts that have to be merged for scientific reasons. In addition, biobanks can support the recruitment of selected patients or test subjects for subsequent research projects only if they use pseudonymous identifiers. It is also the only way to ensure feedback on test results that may be requested by test subjects or patients.

Pseudonyms used for long-term storage should be resolvable only by the smallest possible and narrowly defined group of people. This can be achieved in different ways. In-treatment data collection in the clinical context can be done without any pseudonyms. While the treating personnel enter and view the medical data in direct connection with the identifying data of the patients, in the background the medical and identity data are stored separately and linked together via a "secret" pseudonym. Alternatively, "open" pseudonyms used in the course of the data collection can be replaced by new pseudonyms once the collection and quality assurance have been completed ("double pseudonymisation"). As samples and their genetic information come with an increased re-identification potential, they should not be managed with the same sample number or pseudonym in the biobank and the medical database. A detailed description of different pseudonymisation schemes can be found in the TMF guide for medical research projects [16], which often refers to the 2006 generic data protection concept of the TMF for biobanks [18]. In 2014, the Conference of Independent Federal and State Data Protection Officers recommended to all medical research institutions the use of the TMF guide and the generic data protection concepts described therein. Also part of the coordination with the supervisory authorities is the option of having the TMF's working group on data protection determine to what extent a concrete data protection concept agrees with the generic concepts of the TMF and to what extent deviations from it are to be regarded as critical or unproblematic. Experience has shown that such a determination helps with the further coordination of a concept with the data protection officers of the participating institutions or with the competent supervisory authorities. As this has generated considerable demand, the TMF's data protection working group had to limit the range of advisory services, including the production of a decision, to member facilities of the TMF. However, a simple advisory service continues to be available also for non-members.

These generic data protection concepts also describe what additional technical and organisational measures are necessary to safeguard a long-term collection of samples and data that can be used as widely as possible for medical research. A problem in this context is the necessary openness of such collections for subsequent and not-yet-foreseeable research projects. At best, the affected test subjects or patients can then be asked again to give their specific consent. Often, however, the disproportionate costs involved represent an argument against such re-consent or also dynamic consent. There may also be fundamental scientific or ethical considerations against such re-consent. For example, test subjects' right to not knowing could be violated by a new demand, if their samples and data are to be included in a research project due to a risk factor for dementia – of which the affected parties have had no prior knowledge. Accordingly, other solutions are usually employed today. In order to maintain the principle of informed consent even in such a constellation, the procedure of a subsequent release of the data and samples must be described in detail at the time of consent. In particular, the committee responsible for any subsequent release, as well as all binding decision criteria, must be described and explained in its composition. Since 2003, the TMF has proposed that data controllers set up independent committees for this task and has coined the generic term "Data Protection Committee". Others have suggested the involvement of ethics committees for this task [19, 20]. In this context, in particular, reference should be made to the model consent form for biobanks drafted by the working group of medical ethics committees in Germany, which also follows this principle [7].

It is essential that donors have the right to withdraw their participation verbally or in writing at any time with

or without cause and without adverse consequences. The revocation must be documented by the body that accepts the revocation. In this case, the donor has the right to have his or her data erased and his or her biomaterials destroyed, insofar as this is possible with reasonable effort and if the personal reference of such data and biomaterials has not yet been deleted. In any case, he or she can demand the complete anonymisation of his or her samples and data. Data from analyses already carried out need not be removed [20]. Further references to different utilisation concepts can be found in Siddiqui and Semler [21].

Appointing a trustee has also been envisaged for larger and long-term biobanks as a further protective measure. On behalf of patients, such a trustee manages their identity data and associated pseudonyms and releases these sensitive data only in precisely regulated and carefully examined cases. The necessary independence of the trustee requires regulation-based integration, such as through a cooperation agreement. A mandate-based inclusion as data processing by a processor is contraindicated in this case.

Summary

Even if the requirements of the GDPR are currently highly present in public perception, they are by no means all new. In principle, the requirements of data protection have changed less than the public discourse suggests. However, modified detailed regulations can also be decisive, so that the new requirements must always be studied thoroughly. Unfortunately, this also concerns the federal character of the data protection regulations in Germany, where the GDPR has introduced very little change and as a result can still lead to very different detailed regulations, which must always be examined and taken into account.

The complexity of the regulatory framework and the resulting demands on biobanks only allow for the recommendation to centralise, professionalise and equip such infrastructures with the necessary resources. In line with this, the German BMBF has supported the development of large centralised biobanks and their integration into European infrastructures in recent years through various support measures.

But even beyond such concrete support measures, there are proposals for the networking of biobanks with each other, which should be used in any case in view of the challenges mentioned (with information technology [IT] support requirements and robotics not even having been discussed yet). Here, options, such as those offered by the working groups of the TMF for biobanks and data protection, play an important role.

Author contributions: The author has accepted responsibility for the entire content of this submitted manuscript and approved submission.
Research funding: None declared.
Employment or leadership: None declared.
Honorarium: None declared.
Competing interests: The funding organisation(s) played no role in the study design; in the collection, analysis, and interpretation of data; in the writing of the report; or in the decision to submit the report for publication.

References

1. Schneider UK. Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft, 2015.
2. World Medical Association. World Medical Association Declaration of Helsinki: Ethical principles for medical research involving human subjects. J Am Med Assoc 2013;310:2191–4.
3. WMA. WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks. Taipei: World Medical Association, 2016.
4. Roßnagel A. Kontinuität oder Innovation? Der deutsche Spielraum in der Anpassung des bereichsspezifischen Datenschutzrechts. Datenschutz und Datensicherheit 2018;2018:477–81.
5. Taupitz J, Schreiber M. Biobanken – zwischen Forschungs- und Spenderinteressen. Bundesgesundheitsbl 2016;59:304–10.
6. Simon JW, Paslack R, Robienski J, Goebel JW, Krawczak M. Biomaterialbanken – Rechtliche Rahmenbedingungen. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006.
7. Akmed EK. Mustertext zur Information und Einwilligung in die Verwendung von Biomaterialien und zugehöriger Daten in Biobanken. Recommended by the Permanent Working Party of the German Medical Ethics Committees, approved by the General Assembly on 9 November 2018. Arbeitskreis Medizinischer Ethik-Kommissionen, 2018, Version 3.0.
8. Rammos T. Die datenschutzrechtliche Zulässigkeit von Broad Consent für Forschungszwecke nach der Datenschutz-Grundverordnung. A&R 2017;2017:243–8.
9. BÄK. Medizinische, ethische und rechtliche Aspekte von Biobanken. Berlin: Bundesärztekammer, 2017.
10. Artikel-29-WP. Guidelines on consent under Regulation 2016/679. Brussels: Article 29 Data Protection Working Party, 2018, rev.01.
11. DSK. Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO. Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz (DSK), 2018, Stand: 16.1.2018.
12. Duttge G. Das Recht auf Nichtwissen in der Medizin. DuD 2010;2010:34–8.

13. Jahns R. Errichtung und Betrieb von Humanbiobanken. Ethische Aspekte. Bundesgesundheitsbl 2016;59:311–6.
14. Wollenschläger F. Der Drittbezug prädiktiver Gendiagnostik im Spannungsfeld der Grundrechte auf Wissen, Nichtwissen und Geheimhaltung: Krankheitsveranlagungen im Familienverbund und das neue Gendiagnostikgesetz. Archiv des öffentlichen Rechts 2013;138:161–203.
15. NER. Biobanken für die Forschung. Berlin: Nationaler Ethikrat, 2004.
16. Pommerening K, Drepper J, Helbing K, Ganslandt T. Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF 2.0. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft, 2014.
17. Sariyar M, Schlünder I. Reconsidering anonymization-related concepts and the term “Identification” against the backdrop of the European Legal Framework. Biopreserv Biobank 2016. Epub 2016/04/23.
18. Becker R, Ihle P, Pommerening K, Harnischmacher U. Ein generisches Datenschutzkonzept für Biomaterialbanken (Version 1.0). TMF, 2006.
19. Ethikrat. Humanbiobanken für die Forschung. Berlin: Deutscher Ethikrat, 2010.
20. AKmedEK. Recommendation for the evaluation of research-related biobanks by ethics committees recommended by the Working Group of Medical Ethics Committees according to the resolution dated 10 June 2016. Arbeitskreis Medizinischer Ethik-Kommissionen Deutschlands, 2016, Version 2.0.
21. Siddiqui R, Semler SC. Nutzungskonzepte für Proben und Daten aus humanen Biobanken für die Forschung. Bundesgesundheitsbl 2016;59:317–24.