

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As a rule, data must already be **erased** when the consent is withdrawn.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 With the erasure of the data the data protection law is no longer applicable.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 it 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).