Biobank Oversight and Sanctions Under the General Data Protection Regulation

Dara Hallinan

Abstract This contribution offers an insight into the function and problems of the oversight and sanctions mechanisms outlined in the General Data Protection Regulation as they relate to the biobanking context. These mechanisms might be considered as meta-mechanisms—mechanisms relating to, but not consisting of, substantive legal principles—functioning in tandem to ensure biobank compliance with data protection principles. Each of the mechanisms outlines, on paper at least, comprehensive and impressive compliance architecture—both expanding on their capacity in relation to Directive 95/46. Accordingly, each mechanism looks likely to have a significant and lasting impact on biobanks and biobanking. Despite this comprehensiveness, however, the mechanisms are not immune from critique. Problems appear regarding the standard of protection provided for research subject rights, regarding the disproportionate impact on legitimate interests tied up with the biobanking process—particularly genomic research interests—and regarding their practical implementability in biobanking.

1 Introduction

The oversight and sanction mechanisms are two of the most significant mechanisms in the General Data Protection Regulation (GDPR).[1] Evidence for this might be argued to be found in the extreme build up in data protection compliance activities

[1] European Parliament and Council Regulation (EU) 2016/679 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* O.J. L119/1 (2016). This contribution asserts the applicability of the GDPR to biobanking encompasses all processing of biological samples, all associated genomic, health and lifestyle data as well as any individual level research results. See, for further clarification: Hallinan (2018), pp. 263–295; Hallinan and De Hert (2016), pp. 119–139.

D. Hallinan (✉)
FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur, Karlsruhe, Germany
e-mail: dara.hallinan@fiz-karlsruhe.de

S. Slokenberga et al. (eds.), *GDPR and Biobanking*, Law, Governance and Technology Series 43, https://doi.org/10.1007/978-3-030-49388-2_8

prior, and subsequent, to the GDPR coming into force in early 2016 and applying from early 2018—including in the biobanking context. Some might argue this build-up of activity is due to the substantive novelty of the GDPR.[2] Such arguments, however, are swiftly dismissed with reference to the substantive similarity of the GDPR to its forerunner—Directive 95/46. A much more likely explanation is the increase in data controller compliance activities as a consequence of the fear of oversight potentially leading to novel, and crippling, sanctions.[3]

The astute reader might wonder why these two separate mechanisms fall within one contribution. The answer is relatively straightforward: they go together like salt and pepper. The oversight mechanism functions as the mechanism permitting the generation of information about compliance with the GDPR as well as information about violations of the GDPR. The sanctions mechanism then functions as the dissuasive threat pushing data processing actors towards compliance, which becomes reality—usually—on the back of the oversight mechanism's violation-information generation capacity. The two systems function in tandem in the service of compliance.

The oversight and sanctions mechanisms do not directly define the boundaries of the public interest in biobanking under the GDPR, how the concept relates to other rights and interests or to the conditions under which processing in its service is permissible. Nevertheless, they are indirectly determinative of the concept in two ways. First: as meta-systems ensuring compliance with substantive principles of the GDPR, they are key to maintaining the boundaries, and conditions associated with action in, the public interest in biobanking under the GDPR. Second: the emphasis placed on oversight and sanctions is indicative of the importance the legislator attaches to the need to police and control the boundaries and conditions of the public interest under the GDPR generally.

With the above in mind, this contribution is structured as follows. To start, the chapter provides a descriptive analysis of the function of the oversight and sanctions mechanisms in relation to biobanking under the GDPR (Sects. 2 and 3, respectively). Subsequently, and building on the descriptive analysis, the chapter engages in a critical analysis of the problems raised by the mechanisms. This critical analysis identifies, and considers the severity of, problems from three perspectives: mechanisms' negative impacts on research subject rights; mechanisms' disproportionate impacts on research interests; and mechanisms' practical implementability in the biobanking context (Sect. 4).

[2] See, for example: Kuner (2012), pp. 1–2.

[3] There remains little empirical study of GDPR compliance activity. However, early work very much suggests sanctions are a driving factor in compliance efforts. See: Martin et al. (2019).

2 Biobank Oversight Under the GDPR

2.1 Introduction

The GDPR foresees an extensive, and complex, oversight mechanism relevant to biobanking. This oversight mechanism might reasonably be considered as consisting of four forms—or stages—of oversight: *ex ante* assessment; prior notification and approval; ongoing oversight; and finally, general oversight. The oversight system under the GDPR consists of several oversight bodies. These include those specifically elaborated by the GDPR as well as national bodies such as research ethics committees (REC) and other *sui generis* bodies—for example data access committees. Accordingly, this section will proceed by considering how each of the four forms of oversight foreseen in the GDPR function, before finally considering how the key oversight actors relate to each other.

2.2 Ex Ante Assessment Under the GDPR

Ex ante assessment requires a biobank, prior to engaging in processing, to conduct a Data Protection Impact Assessment (DPIA).[4]

A DPIA is not a general obligation in the GDPR. It will usually, however, be an obligation for biobanks. Article 35(3)(b) clarifies a DPIA will always be required whenever processing includes: 'processing on a large scale of special categories of data'. All personal data processed in biobanking will, as clarified by the Article 29 Working Party, qualify as sensitive personal data by virtue of its planned integration into data driven genomic research.[5] In turn, it seems reasonable that the scale of most biobank projects—even relatively small biobank projects—will already qualify as large scale processing of such personal data.

The base rationale behind a DPIA is the surfacing of information concerning the risks to data subjects' rights and thus to provide an information-base from which to mitigate these risks before processing begins.[6] Where the DPIA obligation is applicable, each aspect of biobank processing falling under the scope of the GDPR must be subject to a DPIA. It is nevertheless possible, however, for one DPIA, to cover 'a

[4] The obligation is outlined in Article 35 of the GDPR. It is true that a DPIA is not oversight in the traditional sense—i.e. an external party checking and confirming behaviour corresponding to some standard. It is, however, so key to the information production process supporting subsequent forms of oversight it might, practically, be regarded as an aspect of oversight.

[5] The Article 29 Working Party observe that all data involved in 'medical research using big data'—such as genomic research—will qualify as data concerning health and therefore as sensitive personal data under Article 9(1) of the GDPR. Article 29 Working Party (2015), p. 3.

[6] See, for example: Van Dijk et al. (2016), p. 289. For more on concrete data subject rights outlined in the GDPR relevant in the biobanking context, please see Ciara Staunton's contribution 'Individual rights in biobank research under the GDPR'.

set of similar processing operations that present similar high risks'.[7] It is logical to conclude that the GDPR permits multiple biobanking operations—even potentially by multiple different biobanks or external researchers—to be subsumed under one single DPIA.

Whilst the GDPR is scant on the procedural and substantive specifics of a DPIA, certain framework conditions are outlined.[8] In particular, the biobank conducting the DPIA must describe processing operations, describe the interests on which the processing is based—where relevant—provide an assessment of the necessity and proportionality of planned processing, offer an assessment of the scale of risks to data subjects and offer an elaboration of steps taken to minimise identified risks. In certain cases—although when exactly remains unclear—a biobank must also seek 'the views of data subjects'.[9] Finally, if any significant change to the proposed processing occurs, the biobanking must go back and review the continued relevance of the original DPIA.[10]

2.3 Prior Notification and Approval Under the GDPR

Prior notification and approval follows, chronologically and legally, from *ex ante* assessment.[11] The prior notification and approval process will tend to involve two types of body under the GDPR. One type of body is specifically elaborated by the GDPR: the Data Protection Authority (DPA).[12] The other type of body will be elaborated by EU Member States following from their obligations to ensure effective safeguards in scientific research under the GDPR.[13] These national bodies will often—although not always, or necessarily—be Research Ethics Committees (RECs).

---

[7] See Article 35(1) GDPR.

[8] See Articles 35(7)(a)-(d) for these conditions.

[9] See Article 35(9) GDPR.

[10] See Article 35(11) GDPR.

[11] See Article 36 of the GDPR.

[12] DPAs are the national authorities tasked with ensuring compliance with data protection law under the GDPR. They are given life and legal base in Article 51(1) of the GDPR. This clarifies that each State must 'provide for one or more independent public authorities'. Whilst being national authorities, DPAs retain independence from national governments. Article 52(1) of the GDPR states: 'Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.'

When biobanking takes place in more than one EU Member State, multiple DPAs may be relevant. In this case, DPAs will collaborate under a specific set of rules. Article 56(1) requires one authority to be designated: 'lead supervisory authority'. This authority will be: 'the supervisory authority of the main establishment or of the single establishment of the controller'. See also: Article 29 Working Party (2016).

[13] See the obligation, in Article 89(1) GDPR, for scientific research to be 'subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject.' See

DPA prior notification and approval is not always obligatory. In fact, it only becomes relevant in two situations. First: Article 36(1) clarifies that advance approval must only be sought whenever a DPIA process: 'indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk'. Significantly, the eventual decision as to whether the prerequisites for notification and approval are fulfilled thus lies, as De Hert and Papakonstantinou observe, with the biobank—although, as will be seen later, in Sect. 2.4, the rationale of this decision is subject to *ex post* checking and verification for compliance with the GDPR.[14] Second: where EU Member States have explicitly clarified that biobanks must consult with the DPA prior to engaging in processing.[15]

When the DPIA has shown a high residual risk or when prior consultation with the DPA is explicitly foreseen in EU Member State law, the biobank must engage in the DPA prior approval process. This process involves the provision to the DPA of all relevant information concerning the planned processing activities. This information will include, in particular, information as to how data protection responsibilities—for example the protection of data subject rights—are distributed between relevant actors, information concerning the 'purposes and means' of processing, information concerning safeguards, DPIA documentation as well as any information specifically requested by the DPA.[16]

Subsequent to DPA checks of information provided, the DPA will then issue the biobank with a decision on the proposed processing. This decision should be available within eight weeks from the start of the process.[17] The decision may take three forms: first, if processing is unproblematic, the DPA will allow it, subject to the conditions of the DPIA, to go ahead; second, if there are specific problematic aspects of processing identified, the DPA will allow it to go ahead only subject to certain conditions;[18] and finally, if processing is irretrievably problematic, the DPA will forbid it in its entirety.[19]

National bodies' prior notification and approval will also not always be necessary. This will depend on whether advance oversight by national bodies constitutes a prerequisite under Member State law. It is not necessarily the case that all Member States require such notification or approval for all, or indeed any, biobanking activity under the GDPR—there is no such comprehensive obligation in the German system, for example.[20] It will subsequently depend on whether national bodies' oversight is required for a specific type of processing. In the UK, for example,

---

also the subsequent chapters in part III of this book on the implementation of Article 89 by EU Member States.

[14] De Hert and Papkonstantinou (2016), p. 192.

[15] See Article 36(5) GDPR.

[16] See Article 36(3)(a)–(e) for lists of types of information to be provided. Article 36(1)(f) includes an open requirement to provide the DPA with 'any other information requested'.

[17] See Article 36(2) GDPR.

[18] See Article 58(2)(d) GDPR.

[19] See Article 58(2)(f) GDPR.

[20] Hallinan (2018), p. 191.

certain biobank activity may be exempted from specific REC oversight under a principle of generic oversight: 'NHS RECs can give generic ethical approval for a research tissue bank's arrangements for collection, storage and release of tissue'.[21]

Where national bodies' prior notification and oversight is necessary, the process and consequences of oversight will depend on the conditions of the relevant body's constitution and the powers bestowed on that body by national law. For example, whilst some REC prior notification and approval mechanisms will require REC approval before biobanking activity can go ahead, this is not universally the case. This is not the case, for example, in relation to the advance oversight procedures of the REC of the Estonian Biobank. According to Article 29(1) of the Estonian Human Genes Research Act: '[the advance] assessment of the Ethics Committee is not binding [in terms of whether processing proceeds]'.[22]

2.4 Ongoing Oversight Under the GDPR

Ongoing oversight—oversight which takes place during processing activity—in the GDPR is carried out by three different types of bodies. Two of these types of bodies are specifically elaborated by the GDPR: the DPA; and the Data Protection Officer (DPO).[23] The final type of body will be—as above—elaborated by EU Member States following from their obligations to ensure effective safeguards in scientific research under the GDPR.[24] As above, these bodies will often—although not always, or necessarily—be Research Ethics Committees.

---

[21] https://www.hta.gov.uk/policies/information-research-tissue-banks. Accessed 4 Mar 2019.

[22] Riigikogu RT I 2000 104 685 *Human Genes Research Act* (2000), Article 29(1). Unofficial English translation available at: https://www.riigiteataja.ee/en/eli/531102013003/consolide. Accessed 4 Mar 2019.

[23] Ongoing oversight is outlined in Articles 39, 57 and 58 of the GDPR. A DPO is an employee of a data controller—or data processor—discussed in chapter IV, section 4, of the GDPR. Despite being an employee, the DPO is required by the GDPR to be allowed to act independently of the interests of their employer. Article 38(3) clarifies: 'The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.' It is true that DPOs are not a mandatory requirement for all data controllers and processors in the GDPR. However, Article 37(1)(c) clarifies that they are obligatory whenever: 'the core activities of the controller…consist of processing on a large scale of special categories of data'. As discussed above, in Sect. 2.2, in relation to the DPIA obligation, this description will cover much biobanking activity. The obligation to employ a DPO may sound like an arduous and expensive one for many biobanking actors. In this regard, it should be noted, perhaps with a sigh of relief, that Article 37(2) allows one DPO to be appointed to represent multiple biobanking actors. The Article specifically allows: '[a] group of undertakings [to] appoint a single data protection officer'.

[24] See Article 89(1) GDPR.

DPAs, in principle, are under no strict requirement to engage in oversight of all, or any particular, biobanking activity. Nevertheless, the GDPR empowers them to engage in specific and detailed oversight of any biobanking activity they see fit.[25] Provided the processing falls within the material scope of the GDPR, there is no limitation to the type of biobank processing—or indeed any other type of data processing—which falls within the scope of this form of DPA oversight. There is, however, little material guidance on how the process of ongoing DPA oversight under the GDPR should look.

If a DPA decides to engage in oversight of biobank activity, the GDPR provides the DPA with investigative powers.[26] These powers include the ability to order the biobanking actor 'to provide any information [the DPA] requires for the performance of its tasks'.[27] If, in the course of an investigation, problems are identified, the DPA is endowed with corrective powers. These powers are wide ranging.[28] They include, for example, the power to order the biobanking actor to bring processing into line with the GDPR.[29] The DPA also has administrative sanctioning powers—these will be discussed later, in Sect. 3.3.

DPOs have a dual function in ongoing oversight. First, the DPO has an advisory role in relation to the biobanking actor. This role requires the DPO to 'inform and advise the…[biobanking actor] of their obligations pursuant to…[the] Regulation and…other…data protection provisions'.[30] Second, the DPO must engage in activities normally associated with external oversight bodies and monitor a biobanking actor's compliance with the GDPR. In this regard, the DPO must: 'monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the [biobanking actor]'.[31]

The biobanking actor is obliged to provide the DPO with all relevant support in the conduct of their oversight activities. This obligation encompasses the obligation to provide the DPO with all necessary financial and administrative support and with informational resources and access privileges.[32] The DPO has no explicit power to remedy any problems they identify. Significantly, the extent to which the DPO is obliged to initiate coordination and collaboration with external authorities—in particular DPAs—in the case of regulatory breach remains unclear.[33]

---

[25] This power is outlined in Article 57(1)(a) GDPR, which states a DPA has the power to: 'monitor and enforce the application of this Regulation'.

[26] These are outlined under Article 58(1) GDPR.

[27] See Article 58(1)(a) GDPR.

[28] See, for example, Article 58(2) GDPR.

[29] See Article 58(2)(d) GDPR.

[30] See Article 39(1)(a) GDPR.

[31] See Article 39(1)(b) GDPR.

[32] See Article 38(2) GDPR.

[33] See, for example, Bergt (2018a). Art. 39, paras 17–20. The consequences of the resolution of this issue are likely to be significant for the role of the DPO in biobanking. In the case the DPO is eventually found to have no DPA collaboration obligation, it seems likely the DPO will become more trusted as a point of data protection reference within biobanks but will also become less

National bodies will have varied capacities in relation to ongoing oversight. As above, this variation will result from bodies' differing constitution and powers under their respective Member States' laws. As above, it is not always the case that Member States will have chosen to require national bodies' ongoing oversight of biobank activity. Even in cases in which they have, it will not always be the case that the relevant national bodies will have the power to conduct ongoing oversight. For example, the Estonian Human Genes Research Act does not task the Estonian Biobank's REC with any form of ongoing oversight.[34]

The process and consequences of national body ongoing oversight will also depend on the conditions of constitution and powers of the national body in the Member State law in question. Most significantly, these conditions and powers will define whether the national body has pro-active oversight capacities comparable to DPAs—or whether they may only react to changes in processing—when they must be consulted in the case of changes in a processing operation and the consequences of their decisions. For example, whilst the UK Human Tissue Act—in Part 2 and Schedule 2—endows the Human Tissue Authority with pro-active oversight capacity, Norwegian law only empowers RECs to be consulted subsequent to changes in biobank processing operations.[35]

2.5 General Oversight Under the GDPR

As opposed to the ongoing oversight process, the general oversight process concerns biobanking activity generally rather than specific biobanking activity.[36] The GDPR foresees participation of two types of oversight body: the DPA; and the European Data Protection Board (EDPB).[37]

DPAs are under no obligation to engage in general oversight. They, however, have the option to engage in general oversight and have the power to 'monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication

trusted by external actors. If the DPO is found to have DPA collaboration obligations, it seems likely the DPO will be less trusted by biobanks as a point of data protection reference but will become more trusted by external entities.

[34] Riigikogu RT I 2000 104 685 *Human Genes Research Act* (2000), Article 29. Unofficial English translation available at: https://www.riigiteataja.ee/en/eli/531102013003/consolide. Accessed 4 Mar 2019.

[35] UK Parliament *Human Tissue Act 2004* (2004), Part 2 and Schedule 2. http://www.legislation.gov.uk/ukpga/2004/30/introduction. Accessed 4 Mar 2019; Storting no. 44 *Act on Medical and Health Research* (2008), Article 11. Unofficial English translation available at: http://www.ub.uio.no/ujur/ulovdata/lov-20080620-044-eng.pdf. Accessed 4 Mar 2019.

[36] The general oversight process is elaborated in Articles 57 and 70 GDPR.

[37] The EDPB is the EU body tasked with providing interpretation and adaptation of the GDPR to ensure the ongoing EU level harmony and suitability of the GDPR. Its composition and function is discussed extensively in Chapter VII, section 3 GDPR.

technologies'.[38] DPAs thus have the power to engage in oversight of biobanking generally, or of specific types of processing activity or technological development which partially overlap with biobanking. As far as DPA interpretations are legal, DPAs may enforce them—see Sect. 3.3, below.

The EDPB also has discretion to engage in general oversight. The key difference between DPA and EDPB oversight is that EDPB oversight operates at EU level. Article 70(1)(e) permits the Board to: '[examine], on its own initiative, on request of [its] members, or…the Commission, any question covering the application of [the] Regulation'. The result will be guidelines or recommendations.[39] These guidelines are technically non-binding. However, they may be difficult for biobanking actors to ignore. As De Hert and Papakonstantinou observe, 'this is a: strong…Board…capable of deciding…and enforcing…opinions'.[40]

2.6 *The Interplay of Actors in the GDPR Biobank Oversight Ecosystem*

As discussed in the previous sections, oversight under the GDPR consists of a mix of both oversight bodies constituted by the GDPR—most importantly DPAs—as well as national oversight bodies served with discharging EU Member States obligations under the GDPR.[41] These national bodies show considerable variation across Europe in terms of form, function and legal constitution. The most important actors are RECs—common across Europe—although these may be joined by *sui generis* legally and non-legally constituted actors—for example data access committees—in relation to specific biobanking activities in specific Member States.[42]

[38] See Article 57(1)(i) GDPR.

[39] See also Article 70(1)(e) GDPR.

[40] De Hert and Papkonstantinou (2016), p. 193. Whilst the EDPB—and its forerunner the Article 29 Working Party—have not yet adopted any guidance specifically targeted to biobanking, they have adopted numerous opinions and guidance documents touching aspects of the applicability of data protection law to biobanking. See, for example, the relevant opinions in the references section of this contribution. Whilst these documents are not always used or followed in Court of Justice of the European Union case law on data protection, they may nevertheless be regarded as significant pieces of guidance on EU data protection law. See their use in, for example: Wachter and Mittelstadt (2019), p. 25. There are three reasons for this significance. First: the EDPB is populated by each of the national DPAs—i.e. the bodies tasked with interpreting and applying the GDPR at national level. Second: the EDPB itself has been given broad powers in interpreting and applying the Regulation to ensure EU level harmony. These powers bolster the normative power of anything the Board says, regardless of its format. Third: EDPB opinions can be issued much faster and with much greater flexibility than CJEU case-law. Accordingly, they cover many phenomena in relation to which CJEU jurisprudence is silent.

[41] See Article 89(1) GDPR.

[42] Expert Group on Dealing with Ethical and Regulatory Challenges of International Biobank Research (2012), p. 43.

Given the lack of homogeneity of national oversight actors across the EU, it is hard to monolithically assert the relationship between actors in the biobank oversight ecosystem under the GDPR.[43] Nevertheless, certain observations might be made.

In the first instance, DPAs will usually enjoy higher legal status than other oversight bodies. This results from their express creation as executive authorities in EU law.[44] As EU law takes precedence over national law, this means DPAs sit above other nationally constituted—by law or otherwise—biobank supervisory authorities in the legal hierarchy.[45] For example, the UK DPA occupies a higher legal status than the UK Human Tissue Authority.[46] The exception to this legal superiority concerns RECs in biobanks linked to clinical trials. Here, the EU Clinical Trials Regulation—for example under Article 4—elevates RECs to the status of EU level oversight bodies.[47]

This hierarchical relationship is normatively significant regarding oversight decisions. Where the hierarchical relationship is in place, if a decision by a DPA concerning problematic aspects of biobank processing contradicts that of another body, the DPA's decision will technically take precedence. Generally, however, it is not the case that a DPA's confirmation that processing is acceptable will overrule another body's decision that processing is problematic. Here, a cumulative logic will apply. For example, if a German DPA finds a biobanking actor's proposed processing acceptable, yet an REC—under Article 15(1) of the Musterberufsordnung für Ärzte—disagrees, processing could not go ahead.[48]

---

[43] In terms of RECs: it should be noted that the form, precise oversight function and legal status of RECs will also vary between EU Member States. For example, in Estonia, they are legally obliged to play a role in the oversight of the Estonian biobank project—although not technically in oversight of other biobanks. Riigikogu *Human Genes Research Act* (2000), Art. 29. Unofficial English translation: https://www.riigiteataja.ee/en/eli/531102013003/consolide. Accessed 4 Mar 2019. In the UK, their legal status in relation to biobanking is much more indirect—secured through institution requirements and executive agency decisions. In terms of other types of biobank oversight actors: in certain Member States, RECs are joined by other, *sui generis* bodies in biobank oversight. In the UK, for example, the Human Tissue Authority—the executive authority responsible for the oversight of the Human Tissue Act—plays a significant role. UK Parliament *Human Tissue Act 2004* (2004), Arts. 13–15. http://www.legislation.gov.uk/ukpga/2004/30/introduction. Accessed 4 Mar 2019.

[44] Indeed, their legitimacy stems not only under the GDPR but also directly—under Article 8—from the Charter of Fundamental Rights of the European Union. European Union *Charter of Fundamental Rights of the European Union*. O.J. C 326/02 (2012), Article 8.

[45] It does, however, seem inevitable that hard cases will emerge in which national oversight entities, constituted by law as safeguards under Article 89(1) GDPR and are better placed than DPAs—in terms of proximity to the object of biobanking oversight as well as in terms of expertise. In such cases, attempts to define hierarchical relationships will likely be difficult and counter-productive.

[46] UK Parliament *Human Tissue Act 2004* (2004), Arts. 13–15. http://www.legislation.gov.uk/ukpga/2004/30/introduction. Accessed 4 Mar 2019.

[47] European Parliament and Council Regulation (EU) No 536/2014 *on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC*. O.J. L 158 (2014), Article 4.

[48] Bundesärztekammer *Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte* (1997 (updated 2018)), Article 15(1). https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/MBO/MBO-AE.pdf. Accessed 4 Mar 2019.

There will be overlap in the oversight tasks performed by DPAs and those performed by other national bodies. This overlap stems, in the first instance, from the broad functionality already taken on by certain biobank oversight bodies. RECs, for example, have traditionally—and will continue to under the GDPR—considered data privacy issues.[49] In turn, in many Member States, the overlap will be exacerbated by the lack of formal clarification of the distribution of oversight tasks among relevant oversight bodies. This duplication of roles may, from a research perspective, be seen as somewhat frustrating. It is not, however, solely a negative—see Sect. 4.3, below, for a discussion of advantages.

How task duplication and division between DPAs and other oversight bodies will precisely function will be context dependent. Nevertheless, it seems likely DPAs will tend toward restraint in scope and means of oversight. This has been documented—at least in the UK context—by Gibbons under Directive 95/46.[50] There seems little reason to think this should change under the GDPR. A number of reasons for this might be proposed. Two seem highly likely: the inaccessible nature—to the layperson at least—of genomic research and limited DPA staff expertise; and the political nature of DPAs and their aversion from interfering in normatively legitimate and publicly supported research—more in Sect. 4.3, below.

One aspect of the oversight relationship between DPAs and other oversight bodies—particularly RECs—under the GDPR is particularly interesting. Anecdotally, under Directive 95/46, many RECs had taken to dealing with data privacy issues by requiring DPA authorizations from biobanks and researchers. Under the GDPR, there is no longer any requirement to gain prior DPA authorisation. Accordingly, this approach will no longer automatically function, and a new approach will need to be sought. In certain cases where no DPA oversight is required, an informal relationship between DPAs, biobanks and genomic researchers, and RECs may develop. In other cases, RECs will simply need to internalise the advance data privacy oversight process themselves.

3 Biobank Sanctions Under the GDPR

3.1 Introduction

In the case that a biobanking actor infringes the substantive principles outlined in the GDPR, two different types of sanctions are envisaged: liability and compensation sanctions; and administrative sanctions. The sanctions mechanism under the

[49] Even if there are doubts as to their efficacy in this regard. See, for example, Dove and his observation that: 'the misalignment of data privacy laws and ethics review boards and committees is an ongoing challenge… [T]hese entities may impose higher standards of privacy protection than privacy laws require… Moreover, there is an inconsistent level or lack of privacy expertise, training, and oversight of many REC members.' Dove (2016), p. 682.

[50] Gibbons (2012), pp. 74–75.

GDPR also fits into a broader biobanking sanctions ecosystem. Accordingly, this section will proceed by considering each of the two forms of sanction foreseen in the GDPR, before finally considering how these relate to the broader biobank sanctions ecosystem.

3.2 Liability and Compensation Sanctions

In order for liability and compensation sanctions[51] to become relevant, a complaint must be lodged. This may happen via the research subject approaching a national court.[52] Significantly, the research subject may choose the location of the court.[53] They may lodge a complaint in their country of residence, or, if the biobanking is located elsewhere, in that country. This may also happen via a research subject mandating a non-profit to approach the national courts on their behalf.[54] However, only non-profits which have been 'properly constituted in accordance with the law of a Member State…[may] lodge the complaint'.[55]

A biobanking actor found liable for causing either material or non-material damage resulting from a violation of the principles of the GDPR will then be liable to pay the research subject compensation.[56] In clarification, the GDPR explicitly includes, in Recital 75, a set of examples of non-material damage. With relevance for the biobanking context, compensation is available for cases in which: 'data subjects might be…prevented from exercising control over…personal data…[or] where [sensitive] personal data are [illegitimately] processed'.

The recognition of the possibility to claim compensation for non-material harm is highly significant in the biobanking context. Laurie et al. had observed that the lack of clarity as to whether this was possible under Directive 95/46 had led, in certain Member States—in the UK, at least—to: 'damage [simply being] equated with financial loss'.[57] Accordingly, before the GDPR, it would have been very difficult for a research subject to obtain compensation for harms concerning, for example, the illegitimate processing of sensitive personal data—precisely the kinds of harms most likely to occur in the biobanking context.

In the case that compensation is found to be payable, the GDPR foresees the possibility for fault to be spread across multiple biobank actors. In this case, the GDPR gives the research subject the power to chase each actor at fault for the complete

[51] Liability and compensation sanctions relevant for biobanking actors are elaborated in Articles 79, 80 and 82 GDPR.

[52] See Article 79(1) GDPR.

[53] See Article 79(2) GDPR.

[54] See Article 80(1) GDPR.

[55] See Article 80(1) GDPR.

[56] See Article 82(1) GDPR.

[57] Laurie et al. (2014), p. 37.

damage.[58] Fortunately, the GDPR also permits any actor held completely liable to recoup any disproportionate losses by chasing other responsible actors for 'compensation corresponding to their part of responsibility for the damage'.[59]

3.3 Administrative Sanctions

In order for administrative sanctions[60] to become relevant, a DPA investigation must be started in one of three ways. First, the DPA itself may begin an investigation—under its ongoing oversight powers, discussed in more detail above, in Sect. 2.4.[61] Second, a research subject may begin an investigation by lodging a complaint with a DPA.[62] Finally, a research subject may also mandate a non-profit to lodge a complaint with the DPA.[63] In the final two cases, the DPA is obliged to investigate the complaint.[64]

In the case that a DPA's investigation finds a violation of the principles of the GDPR, they are endowed with a wide range of administrative sanctioning powers. Certain of these are described as corrective powers—these have been discussed above, in Sect. 2.4. Perhaps most significantly, these include the ability to 'impose a temporary or definitive limitation including a ban on processing'.[65] Beyond these powers, however, DPAs also have the power to impose administrative fines. The scale of these fines is colossal. The power is, as Wybitul puts it: 'drastic'.[66] This power is, arguably, the primary driver of all reaction to the GDPR.

There are two levels of fine relevant for biobanking actors. First level: Article 83(4) outlines fines of '10,000,000 EUR, or…up to 2% of the total…annual turnover' relevant for violations of certain substantive provisions—for example data controller obligations or certification obligations.[67] Second level: Article 83(5) outlines fines of '20,000,000 EUR, or…up to 4% of the total…annual turnover' relevant for violations of other substantive provisions—for example core data protection principles, sensitive data processing prohibitions and data subject rights.[68]

---

[58] See Article 82(4) GDPR. '[E]ach controller or processor shall be held liable for the entire damage in order to ensure effective compensation'.

[59] See Article 82(5) GDPR.

[60] Administrative sanctions relevant for biobanking actors are elaborated in Articles 57, 58, 77, 83 and 84 of the GDPR.

[61] See Articles 57(1)(a) and 58(1)(b) GDPR.

[62] See Article 57(1)(f) GDPR.

[63] See Article 80(1) GDPR.

[64] See Article 57(1)(f) GDPR.

[65] See Article 58(2)(f) GDPR.

[66] Translation by the author of 'drastisch'. Wybitul (2016), p. 203.

[67] See Articles 25–39 GDPR and Articles 42 and 43 GDPR respectively.

[68] See Article 5 GDPR, Article 9 GDPR and Articles 13–20 GDPR respectively.

Fines need not, however, always be imposed at maximum levels. The GDPR provides DPAs with certain leeway in light of the specifics of the case. The GDPR provides, what Schwartz describes as 'a multi-factor test for calculation of administrative fines'. This test—subsequently refined and clarified by EDPB guidance—requires DPAs to consider factors such as the gravity and intentionality of the infringement.[69] In light of such considerations the DPA is permitted to—in relation to minor infringements—waive the fine altogether or impose the fine at discretionary level.[70]

3.4 The GDPR's Sanctions Mechanism in the Biobank Sanctions Ecosystem

There are many sanctioning regimes available for violations of data privacy principles relevant for biobanking actors identifiable across EU Member States. For example, evident in the German context, but in few others, are civil sanctions under Articles 253 or 823 of the Bürgerliches Gesetzbuch for misappropriation of biological samples.[71] Owing to the variety of sanctions and sanctioning regimes operational across Europe, it is not possible to monolithically assert exactly how the GDPR's sanction mechanisms will fit into the biobank sanctions ecosystem. Nevertheless, general observations might be made.

In the first instance, despite DPA discretion and the variety of sanctioning regimes, sanctions under the GDPR are intended to have a harmonizing effect across the EU. This results from the GDPR's nature as an instrument of EU law directly binding in all EU Member States as well as the limited direct capacity for derogation from its sanctions regime. Accordingly, no extensive deviation between Member States is intended. Such deviation would lead to Member States in which conditions for data processing were favourable compared to other Member States—bringing the risk of 'forum shopping'. Whilst the dangers of forum shopping seem rather small in relation to biobanks, the harmonization rationale remains relevant.

Indeed, the need for harmonization in fines has been recently explicitly enunciated by the Article 29 Working Party. In their opinion on administrative fines, they conclude: '[Infringements] should lead to the imposition of 'equivalent sanctions'.[72] They explicitly base this conclusion on the recognition that: 'equivalent sanctions in all Member States as well as effective cooperation between supervisory authorities

[69] Schwartz (2013), p. 1997. See Article 83(2) GDPR.

[70] See Recital 148 and Recital 150 GDPR.

[71] Bundestag *Bürgerliches Gesetzbuch* 1896 (updated 2002), Arts 253 and 283. http://www.gesetze-im-internet.de/bgb/BJNR001950896.html#BJNR001950896BJNG000102377. Accessed 4 Mar 2019.

[72] Article 29 Working Party (2017b), p. 5.

of different Member States is seen as a way 'to prevent divergences hampering the free movement of personal data within the internal market', in line with [one of the core aims of] of the Regulation.'[73]

Regardless of the base harmonization rationale, there will still be instances in which the sanctions for violations of the GDPR's principles in biobanking will differ across EU Member States. Two cases are noteworthy. First, certain public biobanks, in certain Member States may not be subject to administrative fines at all. The GDPR clarifies Member States may limit or exclude fines as they relate to public bodies.[74] Second, supplementary sanctions—beyond those in the GDPR—are still permissible in certain cases. The GDPR clarifies that Member States may define sanctions for violations of the GDPR not already covered by administrative fines.[75] This includes, as Gola observes, the possibility to outline criminal sanctions for biobanking actors.[76]

Despite the above clarifications, it remains unclear just how far Member States can take the possibility to impose supplementary sanctions in outlining sanctions for infringements not covered by administrative fines—in terms of the type of violation which may be addressed as well as the form and degree of sanctions. For example, the relevant Article simply states that Member State sanctions must be: 'effective, proportionate and dissuasive'.[77] There is, however, no common standard regarding this concept. Such vagaries leave considerable room for manoeuvre which will doubtless be exploited by Member States.

Looking across the oversight and sanctions mechanisms, one cannot help but admire their comprehensiveness—at least on paper. Indeed, this comprehensiveness becomes starkly evident when one compares them to many of the alternative oversight and sanctions mechanisms outlined for biobanking—both on international and European level.[78] Despite this comprehensiveness, however, there are problems identifiable with these mechanisms. The most important of these will be discussed in the following section.

[73] Ibid.

[74] See Article 83(7) GDPR.

[75] See Article 84 GDPR.

[76] Gola (2017), Article 84, para 1.

[77] See Article 84 GDPR.

[78] Hallinan (2018), p. 370.

4 Problems with Biobank Oversight and Sanction Mechanisms Under the GDPR

4.1 Introduction

A framework for the critical analysis of the oversight and sanctions mechanisms might consider them from three perspectives: whether they provide adequate protection for data subject rights; whether they disproportionately impact other interests—particularly research interests—tied up with the biobanking process; and whether they are practically implementable in the biobanking context. A critical glance at the mechanisms from these perspectives reveals a number of issues. Three seem particularly worthy of discussion.[79]

4.2 The Lack of Clarity in the DPIA Obligation (Problem 1)

There is much text in the GDPR outlining the DPIA obligation. This is, unfortunately insufficient to remove uncertainty in the biobanking context. As Wright observes generally, the provisions in the GDPR remain 'rather sketchy'.[80] This is a problem of practical implementation.

In the first instance, there remains a lack of clarity about the focus of a DPIA. In particular, it remains unclear whether a DPIA represents another exercise in compliance with the GDPR or whether it represents an effort to go beyond the boundaries of the GDPR's concrete substantive principles to identify and mitigate all potential harms to research subjects.[81] The text of the GDPR seems to suggest the latter, requiring that a DPIA consider and mitigate risks to all 'rights and freedoms'.[82] The practical consequences of this broader approach for the conduct and outcome of, as well as the legal obligations flowing from, a DPIA, however, remain unclear.[83]

In turn, there is a lack of clarity around the method and modalities of a DPIA.[84] Here, four significant issues persist. First, the range of biobanking operations one DPIA may address is unclear. The GDPR explains that multiple similar operations can fall under one DPIA but is silent as to how different operations might be.[85]

---

[79] Problems are dealt with according to the order in which the aspect of the oversight or sanction mechanism to which they relate was dealt with in the descriptive part of the contribution—parts 2 and 3.

[80] Wright (2013), p. 307.

[81] Hallinan and Martin (2020).

[82] See Article 35(7)(c) GDPR.

[83] Ibid.

[84] See, for early reference to the significance of the lack of specificity of the scope of DPIAs in relation to medical research: Fears et al. (2014), p. 4.

[85] See Article 35(1) GDPR.

Second, the precise method to be used to conduct a DPIA is unclear. The GDPR provides some instructions, but these are far from an operationalisable methodology.[86] Third, the effect of a change in processing is unclear. The GDPR requires a review of the DPIA but is silent as to what the consequences of incompatibility should be.[87] Finally, the question of the resources to be invested to conduct an efficacious DPIA remain completely unaddressed.[88]

Finally, there is a lack of clarity as to how the DPIA relates to documentation required by other national bodies' approval processes. Compare, for example, the information and process of a DPIA in the GDPR with the information and process of submission of an application for REC approval under Articles 5–7 of the Clinical Trials Regulation.[89] The overlap is significant—both processes require the production of an outline of the foreseen processing activity as well as a consideration of the foreseen benefits and risks to research subjects. The blunt answer that both processes are legally required is technically correct but substantially unsatisfactory—at the very least, this may require an inefficient use of resources.

Despite the apparently myriad problems, there is reason to think that the lack of clarity in the DPIA obligation will not have a significant impact on in biobanking. Two points are significant. First, a DPIA itself is best considered as an information surfacing process.[90] The substantive impact of an improperly conducted DPIA thus seems likely to be minimal—a DPIA itself will neither ensure or prevent compliance with the GDPR. Second, the DPIA obligation is novel for all actors—biobanking actors and enforcement actors. It thus seems likely that the lack of clarity in the process—including as to how it relates to other assessment processes—will crystalize over time. Until then, it seems unlikely that DPAs or other national oversight bodies will not be too zealous in enforcement.

Equally, the GDPR does facilitate solutions to the lack of clarity in the DPIA obligation both from within and from without. In terms of internal solutions, the GDPR clarifies the EDPB can act to clarify the DPIA obligation.[91] Indeed, the power has already been used in the adoption, by the Article 29 Working Party—the EDPB's forerunner—of DPIA guidelines.[92] In terms of external solutions, both

[86] See Article 35(7) GDPR. There are DPIA methodologies which seek to address this lack of clarity. It is, however, not certain that these are compatible with the GDPR or that the can be effectively used by biobanking actors. See, for example: Commission Nationale de l'Informatique et des Libertés (CNIL) (2015); Information Commissioner's Office (2018).

[87] See Article 35(11). Bieker et al. (2016), p. 24.

[88] Wright et al. (2014), p. 10.

[89] European Parliament and Council Regulation (EU) No 536/2014 *on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC*. O.J. L 158 (2014), Article 4.

[90] Gellert (2017), p. 216.

[91] See Article 64(1)(a) GDPR.

[92] Article 29 Working Party (2017a). The EDPB would do well to look to the DPIA methodology developed in the context of the Datenschutz-Folgenabschätzung (DSFA) für die betriebliche und behördliche Praxis project. The goal of the project is: 'to…refine a process for implementing a DPIA…suitable for different technologies and data processing techniques…equally applicable to institutions of different sizes'. The methodology builds upon that developed by the Forum

Articles 9(4) and Article 89(1) permit EU Member States to enact supplementary conditions clarifying—including in terms of substance, process and relationships to other comparable processes—the DPIA obligation in biobanking.[93]

4.3 The Lack of Obligation to Seek Prior Approval (Problem 2)

As discussed in Sect. 2.3, prior approval by an oversight body is not an obligation in the GDPR. In comparison with international norms this represents an insufficient standard of research subject protection. As will be discussed below, this is a problem for the standard of protection offered to research subject rights.

The obligation to seek prior approval for all genomic research activity may be seen as a minimum standard of research subject protection to be provided by all efficacious biobank law. This is arguable by virtue of the fact the obligation constitutes a norm evident across all biobank relevant international instruments.[94] The World Medical Association Declaration of Taipei states, for example, in Article 19: 'the ethics committee must approve use of data and biological material.'

The GDPR does not explicitly foresee an obligation to gain prior approval from a DPA before engaging in biobank processing. It is true that the GDPR includes provisions on prior approval by DPAs of biobanking processing. These provisions only become relevant, however '[when] a data protection impact assessment … indicates that processing would result in a high risk in the absence of measures taken by the controller'.[95] Recall here the observation of De Hert et al., that the decision as to whether the Article is triggered is eventually with the biobanking actor.[96] It is also true that the GDPR foresees the possibility for Member States to derogate from the GDPR and require prior consultation with a DPA for specific types of

Privatheit project and appears to be the most legally comprehensive and methodologically sound available. https://www.dsfa.eu/index.php/en/home-en/. Accessed 4 Mar 2019.

[93] The wording of the article permits Member States to adopt derogations 'including limitations'. How far this possibility to adopt limitations on the applicability of the Regulations's provisions extends, is not clear. This would be ideally clarified as quickly as possible by the EDPB or by the CJEU.

[94] See Hallinan (2018), pp. 145–146 and the following instruments: Organization for Economic Co-Operation and Development *Guidelines on Human Biobanks and Genetic Research Databases*, 2009. http://www.oecd.org/sti/biotech/44054609.pdf. Accessed 4 Mar 2019; Council of Europe Recommendation CM/Rec(2016)6 of the Committee of Ministers to member States *on research on biological materials of human origin, 2016. Available at* (2016). https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168064e8ff. Accessed 4 Mar 2019; World Medical Association *Declaration of Taipei on Ethical Considerations regarding health databases and biobanks* (2002 (updated 2016)). https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/. Accessed 4 Mar 2019.

[95] See Article 36 GDPR.

[96] De Hert and Papkonstantinou (2016), p. 192.

processing.[97] It remains to be seen, however, how many Member States will implement this requirement.

Nor does the GDPR foresee the obligation to gain prior approval from a national body before engaging in biobank processing. The GDPR does foresee the establishment, at national level, of safeguards for scientific research which may translate into the obligation, in certain Member States, for biobanks to obtain prior approval for processing operations.[98] This may prove a panacea for the issue in future. It does not, however, constitute a panacea now. It is not the case that national body advance approval procedures are comprehensively present in all EU Member States. Even where such advance approval procedures are in place, it is not necessarily the case that they have the power to prevent biobank processing from going ahead. Recall the example of the non-binding nature of the Estonian Biobank's REC decisions.[99]

Despite the apparent significance of the issue, the substantial consequences of the lack of the obligation in the GDPR look likely to be, practically, of diminished significance. Two factors are significant. First: the GDPR will, as discussed above, require prior consultation in certain cases—for example, in cases in which it is uncertain whether risks have been adequately addressed in the DPIA. Second: whilst supporting national oversight bodies are, from a legal perspective, not a panacea in providing a perfect advance approval landscape, their prevalence and efficacy should not be underestimated. For example, whilst certain RECs may not have the power to issue binding decisions on whether biobank processing may proceed, it would also, practically, be highly unusual for their decisions to be ignored.

Equally, the GDPR does facilitate solutions to the issue both via internal and external approaches. In terms of internal approaches: there is no doubt the EDPB could issue guidance highlighting the need to seek prior approval before engaging in biobank processing.[100] In terms of external approaches: Articles 9(4), Article 36(5) and Article 89(1) grant power to EU Member States to elaborate supplemental rules concerning the processing of sensitive personal data in research in relation to the obligation for biobanking actors to seek prior approval from DPAs, other national oversight bodies, or both.

4.4 The Size of Administrative Fines (Problem 3)

The huge size of potential administrative fines outlined in the GDPR is justified based on the need to give data protection law teeth in the face multinational internet companies. This is an image of perpetrator which does not match the majority of

[97] See Article 36(5) GDPR.

[98] See Article 89(1) GDPR.

[99] According to Article 29(1) of the Estonian Human Genes Research Act: '[the advance] assessment of the Ethics Committee is not binding [in terms of whether processing proceeds]'.

[100] Under the power to issue opinions in Article 70(1)(e) GDPR.

public research biobanks at all.[101] As a consequence, for such biobanks, fines are disproportionate. This is a problem concerning the disproportionate impact on interests tied up with the biobanking process.

The reasoning behind the scale of fines—up to 20,000,000 EUR or up to 4% of turnover—makes sense when placed in context. In the legislative process, the scale of fines was discussed as necessary as a deterrent to multinational internet companies' violating the GDPR.[102] Further proof the legislator had this model of target perpetrator in mind when drafting the fines is found in the recognition by certain legal scholars, for example Faust et al. and Bergt, that fines share scale and form with those in EU monopolies law—law concerned with the regulation of cartels and market dominance.[103]

However, the typical public biobanking actor does not compare to such a perpetrator. How then, should such fines be proportionate? Public biobanking actors do not compare in size, financial clout or purpose with large internet companies—or indeed any organisation the target of monopolies law. In this regard, it is enlightening to consider some of the—although admittedly limited—empirical work on the financial constitution of biobanks in the EU. Here, Zika et al. clarify that only 3% of biobanks which answered their large-scale survey were even privately owned.[104] An absurd position: the tiny biobanks of the EuroBioBank rare disease network face the same sanctions as Google.[105]

Despite the potentially crippling, disproportionate nature of fines, there are factors which look likely to, practically, significantly diminish the impact of the problem on biobanking—although the possibility of huge fines will still hang, like the sword of Damocles, above biobanking actors' heads. As discussed in Sect. 3.3, DPAs have significant discretion in setting the quantities of fines. For a number of reasons, it seems unlikely DPAs will ever set maximum—or even near maximum—fines. Quite apart from the fact these would seldom be proportionate, such an act would unlikely be in a DPA's best interest. DPAs operate in a politicised

[101] This will also be true for many private biobanks. There are, however, certain companies building large scale biobanks with huge financial backing and operating with economic imperatives. For such biobanks, the fines seem less disproportionate. See, for example: https://www.23andme.com/about/biobanking/. Accessed 4 Mar 2019.

[102] See, for example, Jan Philipp Albrecht—EU Parliament Rapporteur for the GDPR: 'Companies which violate the new rules must pay fines of up to four per-cent of their yearly turnover. That could be billions for the global internet companies'. Author translation of: 'Unternehmen, die gegen die neuen Regeln verstoßen, müssen Strafen von bis zu vier Prozent ihres Jahresweltumsatzes zahlen, das können für die großen globalen Internetkonzerne Milliarden sein'. Albrecht, Jan Philipp. 2015. Starke Verbraucherrechte und mehr Wettbewerb: EU-Datenschutzreform. https://www.janalbrecht.eu/2015/12/2015-12-21-starke-verbraucherrechte-und-mehr-wettbewerb/. Accessed 4 Mar 2019.

[103] Faust et al. (2016), p. 120; Bergt (2018b), Art. 83, para 2.

[104] Zika et al. (2010), p. 19. http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=3259. Accessed 4 Mar 2019.

[105] http://www.eurobiobank.org/. Accessed 4 Mar 2019.

environment. They are likely to have little appetite to interfere with biobanking activity with normative legitimacy and, as observed by Simon et al., public support.[106]

Equally, solutions to the disproportionate scale of fines are also available through the GDPR as well as parallel law. In terms of solutions available through the GDPR: Article 70(k) is clear the EDPB should: '[draw] up guidelines for supervisory authorities concerning the application of…and the setting of administrative fines'. In terms of parallel law: the flexible construction of Article 9(4)—which specifically permits Member States to enact 'limitations' on the principles of the GDPR in relation to sensitive data—could legitimate Member State derogations restricting the scale of fines relating to biobanking.

5 Conclusion

This contribution dealt with two of the key mechanisms concerning biobanking outlined in the GDPR: the oversight mechanism; and the sanctions mechanism. Indeed, it is arguable that the provisions of the sanctions mechanism—in particular the huge potential scale of administrative fines—are one of the key factors driving the rise in concern for, and efforts toward compliance with, data protection law since the GDPR came into force in early 2016 and since its application in early 2018.

The oversight and sanctions mechanisms play no substantive role in the definition of the public interest—or the conditions pertaining to processing in service of the concept—in relation to biobanking under the GDPR. Nevertheless, they are indirectly determinative of the concept in two key ways. In the first instance, as meta-systems ensuring compliance with the substantive principles outlined in the GDPR, these mechanisms ensure respect for the boundaries of, and conditions attached to, the public interest under the GDPR. In turn, the emphasis on each mechanism acts as an indicator of the level of the legislator's general concern with the ability to police and control the boundaries and conditions of the public interest under the GDPR.

The oversight mechanism in the GDPR applicable to biobanking is—at least on paper—extensive.[107] Indeed, it consists of four types of oversight. First: *ex ante* assessment—the need for biobanking actors to conduct a DPIA. Second: prior notification and approval—the need for certain biobanking actors to obtain approval from a DPA and, potentially, national bodies, prior to processing. Third: ongoing oversight—the need for biobanking actors to submit to investigation by a DPA, a DPO and, potentially, national bodies. Fourth: general oversight—the power for DPAs and the EDPB to issue general opinions on the biobanking sector. It remains,

[106] Simon et al. (2013), pp. 821–831.

[107] Time will tell whether the legislator's presumptions as to the efficacy of the oversight mechanism will play out in practise. Moving forward, biobank oversight under the GDPR looks likely to be a fascinating subject for research.

however, somewhat unclear how the various oversight bodies—in particular DPAs and national bodies—will engage with each other.

The sanctions mechanism in the GDPR applicable to biobanking is also—at least on paper—extensive. The mechanism consists of two key types of sanction. First: liability and compensation sanctions. In the case a biobanking actor is brought before court and found guilty of an infringement of the GDPR, this actor will be liable to pay compensation. Second: administrative sanctions. The range of administrative sanctions available is broad, but perhaps most important are the colossal potential administrative fines—up to 20,000,000 EUR or 4% of turnover. It remains to be seen how the sanctions mechanism explicitly elaborated in the GDPR will fit with supplemental Member State sanctions.

Whilst these two mechanisms display an impressive comprehensiveness in approach, several problems concerning their negative impacts on research subject rights, research interests and their practical implementability to biobanking, are also evident. Three might be highlighted as particularly significant. First: the lack of clarity in the DPIA obligation. Second: the lack of obligation to seek prior DPA approval. And third: the huge scale of potential administrative fines. Although each problem initially seems significant, however, a closer consideration reveals each is subject to practically mitigating factors as well as to resolution through the GDPR, or parallel Member State law, or both.

References

Article 29 Working Party (2015) 'health data in apps and devices', Annex to Communication between the Article 29 Working Party and DG Connect

Article 29 Working Party (2016) Guidelines for identifying a controller or processor's lead supervisory authority. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf. Accessed 4 Mar 2019

Article 29 Working Party (2017a) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Accessed 4 Mar 2019

Article 29 Working Party (2017b) Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237. Accessed 4 Mar 2019

Bergt M (2018a) Art. 39: Aufgaben des Datenschutzbeauftragten. In: Kühling J, Buchner B (eds) DatenschutzGrundverordnung/BDSG. Beck, Munich, pp 753–762

Bergt M (2018b) Art. 83: Allgemeine Bedingungen für die Verhängung von Geldbußen. In: Kühling J, Buchner B (eds) DatenschutzGrundverordnung/BDSG. Beck, Munich, pp 1122–1147

Bieker F et al (2016) A process for Data Protection Impact Assessment under the European General Data Protection Regulation. In: Schiffner S et al (eds) Privacy technologies and policy. Springer, Dordrecht, pp 21–38

Commission Nationale de l'Informatique et des Libertés (CNIL) (2015) Privacy Impact Assessment: methodology (how to carry out a PIA). https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf. Accessed 4 Mar 2019

De Hert P, Papkonstantinou V (2016) The new General Data Protection Regulation: still a sound system for the protection of individuals? Comput Law Secur Rev 32(2):179–194

Dove E (2016) Biobanks, data sharing, and the drive for a global privacy governance framework. J Law Med Ethics 44(4, part. 1):675–689

Expert Group on Dealing with Ethical and Regulatory Challenges of International Biobank Research (2012) Biobanks for Europe: a challenge for governance. https://www.coe.int/t/dg3/healthbioethic/activities/10_biobanks/biobanks_for_Europe.pdf. Accessed 4 Mar 2019

Faust S et al (2016) Milliardenbußgelder nach der DS-GVO: Ein überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz. Zeitschrift für Datenschutz 3:120–125

Fears R et al (2014) Data protection regulation and the promotion of health research: getting the balance right. Q J Med 107:3–5

Gellert R (2017) The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. Eur Data Protect Law Rev 3(2):212–217

Gibbons S (2012) Mapping the regulatory space. In: Kaye J et al (eds) Governing biobanks: understanding the interplay between law and practice. Hart Publishing, Oxford, pp 51–93

Gola P (2017) Artikel 84: Sanktionen. In: Gola P (ed) DS-GVO Datenschutz-Grundverordnung VO (EU) 2016/679 Kommentar. Beck, Munich, pp 756–758

Hallinan D (2018) Feeding biobanks with genetic data: what role can the General Data Protection Regulation play in the protection of genetic privacy in research biobanking in the European Union? VUB Doctoral Thesis, Brussels

Hallinan D, De Hert P (2016) Many have it wrong – samples do contain personal data: the data protection regulation as a superior framework to protect donor interests in biobanking and genomic research. In: Mittelstadt B, Floridi L (eds) The ethics of biomedical big data. Springer, Basel, pp 119–139

Hallinan D, Martin N (2020 Forthcoming) Fundamental Rights, the Normative Keystone of DPIA. European Data Protection Law Review.

Information Commissioner's Office (2018) Sample DPIA Template. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf. Accessed 4 Mar 2019

Kuner C (2012) The European Commission's Proposed Data Protection Regulation: a Copernican revolution in European data protection law. Priv Secur Law Rep 11:1–15

Laurie et al (2014) A review of evidence relating to harm resulting from the uses of health and biomedical data. http://nuffieldbioethics.org/wp-content/uploads/FINAL-Report-on-Harms-Arising-from-Use-of-Health-and-Biomedical-Data-30-JUNE-2014.pdf. Accessed 4 Mar 2019

Martin N et al (2019) How data protection regulation affects startup innovation. Working Paper

Schwartz P (2013) The EU-U.S. privacy collision: a turn to institutions and procedures. Harv Law Rev 126:1966–2009

Simon C et al (2013) Active choice but not too active: public perspectives on biobank consent models. Genet Med 13(9):821–831. https://doi.org/10.1097/GIM.0b013e31821d2f88

Van Dijk N et al (2016) A risk to a right? Beyond data protection risk assessments. Comput Law Secur Rev 32(2):286–306

Wachter S, Mittelstadt B (2019) A right to reasonable inferences: re-thinking data protection law in the age of inferences and big data'. Columbia Bus Law Rev 2:1-130.

Wright D (2013) Making Privacy Impact Assessment more effective. Inf Soc 29:307–315

Wright D et al (2014) A guide to surveillance impact assessment — how to identify and prioritise risks arising from surveillance systems. SAPIENT Project Deliverable 4.4. https://zenodo.org/record/1182874#.Wpf3RqjOXIU. Accessed 4 Mar 2019

Wybitul T (2016) Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte? Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen. Zeitschrift für Datenschutz 5:203–209

Zika E et al (2010) Biobanks in Europe: prospects for harmonisation and networking. http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=3259. Accessed 4 Mar 2019