Abstract  Insights into the incidence and survival of cancer, the influence of lifestyle and environmental factors and the interaction of treatment regimens with outcomes are hugely dependent on observational research, patient data derived from the healthcare system and from volunteers participating in cohort studies, often non-selective. Since 25th May 2018, the European General Data Protection Regulation (GDPR) applies to such data. The GDPR focuses on more individual control for data subjects of ‘their’ data. Yet, the GDPR was preceded by a long debate. The research community participated actively in that debate, and as a result, the GDPR has research exemptions as well. Some of those apply directly; other exemptions need to be implemented into national law. Those exemptions will be discussed together with a general outline of the GDPR. I propose a substantive definition of research—absent in the GDPR—which can warrant its special status in the GDPR. The debate is not over yet. Most legal texts exhibit ambiguity and are interpreted against a background of values. In this case, those could be subsumed under informational self-determination versus solidarity and the deeper meaning of autonomy. Values will also guide national implementation and their interpretation. The value of individual control or informational self-determination should be balanced by nuanced visions about our mutual dependency in healthcare, as an ever-learning system, especially in the European solidarity-based healthcare systems. Good research governance might be a way forward to escape the consent or anonymise dichotomy.

© 2018 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
1. Introduction

After a long discussion, the General Data Protection Regulation (GDPR) [1] was finalised in May 2016 and became applicable on 25th May 2018. The position of health research with data played an important part in the discussion till 2016. In general, the GDPR strengthens individual control of data subjects over their data in this digital age. Regarding research, the European Parliament (EP) took that to the extreme with a ‘consent or anonymise’ approach in its 2014 version of the draft GDPR [2] in spite of existing criticism in the literature about that approach [3]. Worried comments from researchers and patient organisations followed [2,4–7]. The Wellcome Trust with the website data-saveslives (now with a different content) [8] has been extremely helpful in bundling efforts. Andersen and Storm showed how the use of anonymised data as an escape to consent led to unreliable results for the German cancer registries, affecting research integrity [9]. These efforts were successful as the final version of the GDPR became more nuanced, albeit with two downsides as well. The ‘trialogue’ [2] between European Commission, EP and the Council did not reach full harmonisation regarding clauses in the GDPR which in the context of scientific research contains an exception to the general regime of the GDPR. Many of these research exemptions have been left to the member states. In addition, the GDPR shows considerable ambiguity between individual control and the concept of ‘public interest’ as a counterbalance when appropriate [10].

In part 1 of this article, the GDPR as it stands now will be discussed. This involves choices. With its 99 articles and 173 recitals, which are important for the interpretation of the articles, the GDPR is a complex piece of legislation. That complexity is increased by the often vague terms. This article cannot offer an annotated version of the GDPR, and hence, some general remarks or highlights must suffice. Choices have been largely made based on a presumption about the endurance of the readers of this journal to digest legal texts and what researchers and doctors need to know to contribute to discussions on the values and principles of observational research. The organisations in which they are embedded need to take measures for compliance as well. Those remain largely out of scope in this article. Although still too brief for thorough lawyers, I want to avoid the pitfalls of ignoring the complexity or show a biased reading of the GDPR [11]. The GDPR does not equate data processing for healthcare and research with that of social media such as Facebook.

The background and underlying values of the debate will be sketched briefly in section 3. Other perspectives are possible than the infamous ‘consent or anonymise’ dichotomy and the ‘fetishisation of consent’ [3].

2. The GDPR as it stands in autumn 2018

2.1. The general principles of the GDPR

Principles will be taken wider here than those mentioned in article 5 of the GDPR. See Textbox 1 for an abbreviated version of those principles. In addition to those,

- one should have a legal basis to process personal data in general (article 6);
- one should have a specific legal basis to process sensitive personal data, such as data about health (with a broad meaning) and genetic data (article 9);
- transparency about data processing (articles 13–14);
- data subjects have rights to their data, such as access, rectification or erasure, restriction of processing, a right to object and data portability. Those rights are subject to various restrictions, under which research exemptions (articles 15–22);
- data protection by design and by default (article 25);
- data processing should be secure (article 32).

2.2. The legal basis

The GDPR also introduced huge fines for infringements on the GDPR which may have contributed to a sometimes overcautious interpretation. Around May 2018, an avalanche of emails asks for consent to remain on mailing lists while actually such consent might not have been necessary. Consent is certainly not the only legal basis for processing personal data, and for having one’s mail address, the sender should have had a legal basis already. The GDPR is the successor of the Data Protection Directive (DPD) of 1995 which required a legal basis to process personal data as well. Regarding legal bases to process data in general, actually nothing has changed, except that government cannot use the last resort clause anymore, being the legitimate interest of the ‘data controller’ (Textbox 2) insofar as the privacy interests of the data subjects do not outweigh those interests (6.1.f GDPR). The EU legislator considered that a governmental body should be able to fall back on one of the other bases, being for example a legal obligation

Textbox 1. General principles of GDPR

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality.

In: van Veen, Eur J Cancer 2018; n: ....
Textbox 2. What is a data controller according to GDPR?

The data controller is the entity that decides about purposes and means of data processing. A data processor is an entity that, although not belonging to the organisation of the controller, processes data on behalf of the controller such as a cloud services provider. The processor does not need a legal basis in article 6 or 9 GDPR. A controller–processor agreement is required (article 28 GDPR).

In: van Veen, Eur J Cancer 2018;

(6.1.c) or a task in the public interest or an official authority (6.1.e).

To process sensitive data, the controller should have a specific legal basis, in addition to article 6. In principle, the processing of such data ‘shall be prohibited’ (9.1 GDPR). This is astonishing as all health and social care and much more would cease immediately. The second section of the article mentions the exceptions to this prohibition. The first exception is the explicit consent of the data subject unless a specific law states that the prohibition cannot be lifted by explicit consent (9.2.a). In some EU countries, the latter would pertain to direct to consumer genetic tests [12] or medical examinations for private life insurances [13]. Just as in the case of article 6, the list is longer than consent. In Textbox 3, the exceptions to the informed consent principle relevant for healthcare and health research are summarised.

Textbox 3. Exemptions to informed consent specifically for processing health data in the context of health services and research

- Necessary to protect the vital interests of the data subject (9.2.c);
- Necessary for preventive or occupational medicine, ...medical diagnosis, provision of healthcare etc. based on member state or Union law and subject to professional secrecy (9.2.h and 9.3);
- Necessary for the public interest in public health, such as protection against serious cross-border health threats, assuring high standards of quality and safety etc ... on the basis of Union or member state law when suitable safeguards for the rights and freedoms of the data subject are provided (9.2.i);
- Necessary for scientific, historical or statistical purposes in accordance with article 89.1 (see text), based on Union or member state law which must be proportionate to the aim pursued and provides suitable and specific measures to safeguard the rights and freedoms of the data subject (9.2.j).

In: van Veen, Eur J Cancer 2018;

2.3. Directly applicable research exemptions

The GDPR contains some directly applicable research exemptions. These are summarised in Textbox 4.

The principle of article 5.1.b is very important. It was already in the DPD (article 6.1.b) yet subject to national implementation. It means that if a controller further processes its ‘own’ data for research or statistical purposes, it does not need a new legal basis for this ‘further use’. The original legal basis suffices. Yet, this does not mean that those who do not have access to the personal data for reasons of medical confidentiality can now have

Textbox 4. Directly applicable research exemptions in GDPR

- Purpose limitation, article 5.b

Personal data should be processed in a manner that is compatible with the original purpose. Further processing for scientific research or historical research purposes is not incompatible with the original purposes for which these data were collected.

- Storage limitation, article 5.1.e

Personal data should not be kept in a form that permits the identification of subjects longer than is necessary for the purposes of processing except if longer storage is necessary for scientific research purposes and in accordance with article 89.1 (see text) and when subject to appropriate technical and organisational measures.

- Transparency when data have not been obtained from the data subject, article 14

14.5.b: Not if provision of such information would be a disproportionate effort, such as for scientific research but subject to the conditions and safeguards of art. 89.1 or in so far as disclosure would render impossible or seriously impair the objectives of the processing. In such cases, appropriate measures must be taken.

- Right to erasure (right to be forgotten), article 17

Does not apply:
- 17.3.c: For reasons of public interest in the area of public health pursuant to art 9.2.h and i.
- 17.3.d: For research in accordance with art 89.1 and insofar as research would be seriously impaired or rendered impossible.
- Right to object, article 21

Several grounds for the right to object to data processing.
Research as such is not one of them in the directly applicable exemptions.
However: right to object against processing personal data for research does not apply if processing is necessary for a task carried out in the public interest (article 21.6).

access [14]. And, if the personal data would be transferred to another legal entity to perform research, that new controller would need its own legal basis.

2.4. Research exemptions that need implementation into national law

Other research exemptions, in addition to those mentioned in Textbox 1 (articles 9.2.i and 9.2.j), require implementation into national law. Those are summarised in Textbox 5.

A more detailed list and explanation of the directly and indirectly applicable clauses can be found at http://www.medlaw.nl/nieuws/gdpr-and-research/[15].

2.5. Personal data

The GDPR applies to personal data, not to anonymous data. Just as under the DPD, personal data are also data that are indirectly identifiable. The bar is high to consider data which in an earlier phase of their lifecycle were personal data and anonymous data at a later stage after certain transformations of the data. Yet, as follows from the Breyer decision of the European Court of Justice in October 2016, the risk of re-identification does not need to be zero. The Court states data can be considered anonymous ‘if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant’ [16]. This is a more nuanced view than that of the article 29 Working Party, now the European Data Protection Board (EDPB), in its 2014 Opinion on anonymisation techniques [17].

Although the decision of the Court was given under the DPD, it also applies to the GDPR. The definition of personal data did not change. More examples were added in the definition and Recital 26 of instances which could lead to identification. It should be mentioned that the proposal of the EP to consider all individual-level data (‘singling out’) personal data did not make it to the final text. Singling out remained in Recital 26 as an example which can more easily lead to identification.

The new ISO document on anonymisation carefully shows the trade-offs between various anonymisation techniques and their—in short—usability for research purposes [18]. Anonymous data to the highest standards without any residual risk for re-identification lose their value for nuanced research [19,20]. Methods such as ‘data-shield’ [21] or VIPAR [22] claim to bring the questions to the data and hence be able to avoid the complexities of data protection rules. However, data-shield methods are only applicable to databases that are formatted for research, containing large volumes of data. It is as yet not applicable to electronic healthcare records or research with scarce data as in the case of rare diseases.

There is considerable debate whether data that should be considered personal data when released in one context, such as ‘open data’, to the public, can be considered anonymous data if processed in the context of a safe data environment [23–26].

However, what matters most is the following. Contrary to what is often thought, being in short, ‘anonymous data are free’, anonymisation, even if feasible, does not solve all governance issues of health research. Also, the earlier consent, the path to [27] and the use of anonymous data should follow the good research governance principles as briefly described in the following.

2.6. Pseudonymised data

The GDPR has introduced a definition of pseudonymised data and states that data according to that definition are personal data (article 4.5). This has already often led to the misunderstanding that all ‘pseudonymised data’ are now personal data [27]. The definition of the GDPR states that pseudonymised data are data where the key to the more identifiable data under the pseudonym is safely kept by the controller. In principle, that controller can reverse the pseudonym back to the identifiable data behind it. Especially in the Netherlands [19,27], the term pseudonymisation has also been used for a step in the data chain from the controller to a research database in which the pseudonym is configured by a trusted third party via a one-way hash, hence an irreversible pseudonym. That procedure does not lead to pseudonymised data in the sense of the GDPR. So we might have to use a new word for it, such as ‘one-way key-coded data’.

Whether that procedure leads to anonymous data is yet another question. That will depend on the safety of the pseudonym and the indirect identifiability of the
data under the pseudonym, when they are released from the data provider and, more importantly, when they are combined in the research database under the pseudonym.

2.7. Informed consent under the GDPR

The GDPR raised the bar for consent. Recital 32 and article 4.11 give a definition, being freely given, specific, informed and unambiguous by a clear affirmative act. Article 7 of the GDPR states the conditions for this consent to be valid. It must be demonstrable and should be detached from other matters for which data processing is necessary, such as a contract. It may be withdrawn at any time although that shall not affect the lawfulness of the processing before the withdrawal.

The ‘specific’ will be discussed infra. The ‘free’ needs further clarification here. Basically it means that if one cannot participate in a certain activity, which is not about data processing as such but requires data processing to be performed, there cannot be free consent for the data processing necessarily inherent to that activity. The consent and the legal basis for data processing should then shift to the—informed—consent to participate in that activity. Related to healthcare, it goes without saying that, except in emergency situations, all diagnostic and interventional procedures in healthcare should be based on informed consent of the patient. In that case, the data processing that is inherent to these procedures is based on the informed consent to undergo the procedure. The legal basis will then be the national legislation about the healthcare provider–patient relation. The legal basis is not informed consent to process personal data in the sense of articles 7 and 9.2.a of the GDPR. The rest of the GDPR will still apply such as transparency about the data processing (article 13, applying to all legal bases). And, if additional questions would be asked in the context of a treatment, such as for Patient Reported Outcomes Measures (PROMs), then processing should be based on informed consent, hence article 9.2.a.

Applied to research, a distinction appears. If the research is an observational study that starts with participants filling in questionnaires, the basis would be consent in the sense of article 7 and 9.2a. But, if the study would be a clinical trial in the sense of Regulation 536/2014 (CTR) [28], the data processing would not be based on consent in the sense of article 7 and 9.2.a. Regulation and the Good Clinical Practice rules [29] contain detailed provisions about the data processing inherent to participating in a clinical trial and the compliance of those involved in executing the trial. One cannot give informed consent to participate in a clinical trial and at the same time refute the data processing which follows from the CTR. The legal basis would be 9.2.h (see Textbox 1), in this case not national law but EU law.

The CTR recognises that the data collected in the context of the trial protocol can also be used for scientific research outside that protocol. In that case, the data protection law will kick in (article 28.2 last sentence of the CTR). Recital 29 of the CTR states that informed consent is needed (9.2.a GDPR), but there might also be other legal bases for such ‘further use’.

2.8. Broad consent

Recital 33 recognises to some extent ‘broad consent’. This Recital has been added in the final text of the GDPR and shows some ambiguity. ‘The specific purposes of data processing for research cannot be fully identified at the start of data collection. Therefore, data subjects should be allowed to consent for certain areas of research’. Recognised ethical standards should be met and insofar as allowed be the intended purpose (my emphasis), data subjects should have the opportunity to narrow their consent.

This could pave the way for broad consent, as has been the norm in biobanking and data sharing based on the FAIR (findable, accessible, interoperable and reusable) principles [30], but there is opposition to this clause as well (section 3.2).

2.9. Article 89.1

Many articles in the GDPR concerning research refer to article 89’s first paragraph. See the longer explanation on the internet for the text [15]. In essence, this article repeats the principles of data minimisation and privacy by design and default. Under the name ‘privacy-enhancing principles’ (PET), these principles were already discussed in 2008 [31], further elaborated by discussing ‘privacy zones’ [32] and in the context of ‘safe research data havens’ [20].

Hence, while these principles are not actually new, not all researchers may have been aware that part of their licence is using solid methodological justification why certain data of a certain type are needed in a specific phase of the research, balancing that justification with the privacy interests of those involved. Article 89.1 emphasises this. It does not forbid to process certain kinds of data or states that only pseudonymised data can be used.

2.10. The data protection impact assessment

New in the DPR is the requirement of a ‘data protection impact assessment’ (DPIA) if among other things, large amounts of sensitive personal data are being processed (article 35 GDPR). It should be assumed that a DPIA is necessary for every major research project with health data. Yet, one DPIA can cover similar projects (article 35.1) The DPIA should assess the risks of the data processing and describe how these risks will be averted.
The DPIA is first of all a self-assessment together with the data protection officer and taking the views of the data subjects into account (article 35.9). In the context of health research, this means in liaison with patient organisations. If there is doubt whether the risks can be sufficiently averted, the national data protection authority should be consulted (article 36). The then article 29 Working Party, now the EDPB, gave guidance on when and how a DPIA should be executed [33].

2.11. Registers and research

As is shown by other articles in this issue [34,35], cancer registries and their ‘fruits’ [36] are of paramount importance for monitoring cancer incidence and survival as well as for research purposes. In the same vein, they are essential to evaluate cancer-screening programs [37]. Recital 157 stresses the importance of registries. ‘By coupling information from registries, researchers can obtain new knowledge of great value …’. This recognition is a great improvement compared to the DPD but can only be seen as incentive for national legislation. The GDPR does not contain a directly applicable exemption to the informed consent principle for registries. Registries will have to be based on national law implementing article 9.2.i. As with informed consent, they would become unreliable due to bias [38–41] or even ‘die’ [42]. If they would claim to process only pseudonymised anonymous data, they would generate unreliable data as well [9].

2.12. International cooperation: towards a rule of recognition

Different national implementation of the research exemptions may lead to problems in international research projects. It might seem impossible for certain centres to participate as ‘their’ data cannot be released for the project. Yet, most of these problems can be addressed. Federated data systems where the data are analysed on the spot according to a single protocol and often data harmonisation in between [43] can offer an alternative. However, such federated systems are not always feasible, and ultimately one research database vested in one member state needs to be created. Then, a ‘rule of recognition’ should apply [44,45]. This means that the sending country cannot prohibit data to be sent to a country with a more lenient regime regarding the research exemptions. Vice versa, a receiving country with a more strict regime cannot prohibit the processing in that country of data which have been assembled for research in a country with a more lenient regime. In both instances, obviously only if the restrictions on the use of these data by the data provider continue to be applied during data analysis in the research database. This was assumed to be a general European law already, and article 1.3 of the GDPR corroborates that view. This article states that ‘the free movement of data within the EU shall not be prohibited for reasons connected with the protection of natural persons with regards to the processing of personal data’. It should be remembered that issues such as data safety and privacy by design are not dependent on national legislation but are directly applicable, whether a member state has implemented the research exemptions more broadly or more restrictively.

The GDPR explicitly recognises joint controllers (article 26). Joint controllership for research data can be a possibility within one country but should remain manageable and transparent. I propose around 7 as a guideline. Beyond that and with controllers from member states with different background regimes, joint controllership becomes unmanageable and insufficiently transparent for the data subjects. In that case, the custodian of the centrally assembled research data should be the sole controller, and data transfer agreements (DTAs) should regulate the processing through that database. The data protection officer of the receiving centre should assure that the conditions are indeed met, next to potential other governance mechanisms of the project such as decision procedures about the use of the database for specific protocols when applicable.

2.13. Research and the public interest

Research is not defined in the GDPR and neither is public interest. Recital 159 states that research should be interpreted in a broad manner, including fundamental and privately funded research. Recital 159 refers to to article 179.1 Treaty of the Functioning of the EU, which among other things stresses research as a means for EU to become more competitive in the global market, also commercial research can be subsumed under research as meant in the GDPR.

The specific position of research in the GDPR indicates that research as such is in general considered to be in the public interest. Yet, to legitimise this licence with clauses that derogate from the general regime of data protection and hence fundamental rights, a more substantial and normative definition is needed. In the earlier internet publication of this article [15], a set of criteria was mentioned which—in italics—has been added to with later insights:

I. Research lead to generalisable results of the object of investigation and is performed according to the accepted methodological standards [46].

II. The data processing for research is as such not meant to lead to decisions about specific data subjects. There will always be a ‘translation’ of these results into daily practice.

III. Research is as much as possible reproducible.

IV. Research adheres to recognised standards of research integrity [47,48].
V. The results will always be published in the public domain (which can mean scientific journals with payed access).
VI. The underlying data will be FAIR [30].

These criteria overlap and even go somewhat further than the criteria for ‘bona fide research’ and the departments which perform the research as discussed by Floridi et al. [49]. The background of that article is the Innovative Medicines Initiative (IMI) [50] projects where academia and industry cooperate in approved, often very-large-scale projects. Industry does not have an impeccable track record in transparency about data, and the danger of ‘conflict of interests’ is imminent [51–54]. Hence, the ‘bona fide’ and also another more substantive criterion are added:

VII. There should be a justification that this research can contribute to the public interest. This means in the field of health that it may improve a better understanding of underlying mechanisms leading to ill-health or to better options for prevention or treatment.

These seven criteria will guide the discussion in the next section.

This definition of research does not necessarily coincide with ‘public interest’ in the text of the GDPR. When the GDPR mentions public interest and research in the same sentence, it rarely does so as a combination. Except for article 21.6 (Textbox 4), there is always a comma between ‘public interest’ and ‘research’, indicating that they are separate legal bases. The ‘public interest’ in the text of GDPR presupposes a democratically accountable public body that has assigned an activity specifically in the public interest. Research might not always be in the public interest in that specific sense. Research may go against the current. That is also the public interest in the general sense, if we accept an ‘open society’ and a general, more substantive concept of ‘public interest’ which may not always coincide with majority views [55,56].

The GDPR contains a clause about the freedom of expression and information which is not research according to those 7 criteria (article 85). That freedom, important as it is, has much fewer ramifications in the rest of the GDPR and is much more dependent on national implementing legislation.

3. Reflections on the future of the debate

3.1. Introduction

With the last section, the debate about the licence for research with health data was introduced already. That research meeting the seven criteria is a necessary but not a sufficient criterion. Ethical vetting of research protocols has not been discussed and is a necessary condition as well. However, the main future discussion will revolve around consent and governance by (as opposed to how they are governed, the governance of) research projects.

3.2. Consent and its dissidents

As mentioned, the thrust of the GDPR is to give data subjects more control over their data. Consent is the paramount paradigm according to many. It is reflected in the Guidelines of the former article 29 Working Party on consent [46] and transparency [57]. The Guidelines on consent downplay Recital 33 to the point of becoming nearly non-existent and hence showing an anti-democratic tendency as the legislator inserted that clause in the final text with a purpose. The Taipei Declaration [58] of the WMA calls for consent even for registries. Recently, the democratic legitimation of declarations of the World Medical Association (WMA) and the Council for International Organisations of Medical Sciences (CIOMS) was challenged [59], reflecting in much more sophisticated ways reservations about this international quasi law making already in 2004 [44]. The swift rebuttal to this critique [60] misses the point. It does not discuss how alternative views were taken up in this seemingly self-referential system of experts appointing each other. A somewhat similar critique could apply to the EDPB. The meta-governance debate—about the governance of the governance of research—would require more discussion however.

More linked to the research community is the quest for ‘dynamic consent’ [61,62]. Originally meant for research projects with active participants dynamic consent now seems to be extended to research with anonymised data from electronic healthcare records [63]. In that case, the bias problem [38–41] would certainly kick in. In addition, it is unclear how dynamic consent copes with the situation when the full blown options to steer information have been ticked, but after a while, the participant does not respond to the alerts.

The critiques have different perspectives. The more practical perspective starts with consent as a basis and discusses how it cannot steer informational self-determination in big data analyses [64] or further disclosure following the FAIR principles [65].

At a more fundamental-level ‘informational self-determination’, as such is challenged. In the context of biobanking, our responsibility for future generations is proposed in the same way as that for the environment [66]. Others have emphasised solidarity in the context of ‘further use’ of health data for research [19,67]. In the context of opening data from healthcare records for research, an argument is made for a duty of rescue if that can be done at minimal risk for the person concerned [68]. There is critique on the ‘my data’ approach to patient data as these have originated from the professional standard, based on research and practical experience of many before this particular patient and the purely medical data—as opposed to the personal account of the patient—should relate to every patient with a similar condition [19].
Such arguments cannot be ‘stapled’. They start from different moral perspectives and have different provisos and different consequences, although they underlie a new trend in ethics, as discussed in 2005 already [69].

Perhaps the most fundamental critique of the pro-consent movement would be as follows. It might be caught by an internalisation of the lure of affluent choice and how we can and even should fulfill our wishes which has permeated neoliberal society [70,71] and misapples that for ‘autonomy’ [72], undermining social institutions [73] such as healthcare, which rather need a ‘we’ approach than a ‘me’ approach [74].

As a final caveat to this section, the above should not be read as a disapproval of consent for ‘further use’ of data as a fundamental aspect of respect. Always, ‘further use’ as a means to improve healthcare should be made explicit and when feasible, also considering the bias problem, consent should be asked. An opt-out option should always be open, if only to guarantee accessibility to healthcare [19] but also as a means of ‘voice’ when trust is undermined.

3.3. The ‘governance by’

Here, we turn to how this ‘further use’ and research projects should be governed by those involved in managing these projects. This section must be extremely brief. After a first crude attempt in this Journal in 2008 [31], O’Doherty et al. proposed governance mechanisms for biobanks under the heading ‘From consent to institutions’ [75]. Although seminal, their deliberative approach is not always feasible in larger scale projects with a less defined constituency. The thrust is to align with patient organisations and the public in general [20], to explain, to listen and to adjust to that feedback and be accountable. This also requires full transparency and an opt-out option also at later stages, insofar as the data can still be traced back, when trust would be undermined by data breaches or other negative publicity. These principles also apply to projects that claim to contribute to ‘public health’, of which there are many examples in this issue. The concept of public health is not without its own quandaries [76].

This brief sketch of governance by researchers assumes application of the aforementioned substantive definition of research, thus not covering everything. The downstream effects of drug development and whether the liaison of academia and pharma will result in fair pricing [77] and promotion of drugs [78] are not covered by upstream agreements about that liaison. Neither does it apply to liaising of healthcare providers and researchers with software firms to develop decision support systems [79].

Yet, those wider issues cannot just be solved through consent but rather through collective mechanisms of governance of those actors against a background of existing or possible government interventions.

3.4. The debate continued

The H2020 Aegle project provides among other things insights into the national implementation [80]. The European organisation for biobanking, BBMRI-ERIC, has initiated a European Code of Conduct for health research with data [81,82], which may result in more harmonisation [10]. It certainly might do so in giving guidance on many of the ‘vague’ terms of the GDPR. But, the underlying values remain reflected in the discussions. Given the present stakes [see also 83,84] this discussion might not so easily be resolved as when Toulmin and others participated in a presidential Committee in the USA to issue guidelines on research with human subjects [85].

4. Concluding remarks

These are interesting times for the health research and patient communities. The Organisation for Economic Co-operation and development (OECD) called for ‘opening up the silos’ where health date are kept [86]. Health research will be able to tap into an increasingly wide range of data sources, including mobile devices [87]. The European Commission published a communication calling for an ambitious program on prevention and health research by combining data [88], many IMI and H2020 projects being underway. Yet, all that data processing must also be channelled through the GDPR and, in the context of health data, registries and research, its national implementation. This article provides researchers with better understanding not only of the GDPR but also about the underlying values. The future of biomedical research in Europe will be decided not only by the GDPR text but also by the outcomes of the debate on those values. The brief sketch of ‘governance by’ made a strong call to liaise with patient organisations and the public at large, not only to explain what this data exchange for a learning healthcare system is all about but also to listen to the feedback and have a more community-centred research agenda.

Observational research with health data needs to be unbiased, or it will mislead care providers, policymakers and patients alike. The data processing should also reflect the values embedded in the GDPR. The downstream applications should contribute to a just society. Regulators, lawyers, ethicists, researchers, care providers, patient organisations and the public must remain in a constant open dialogue to safeguard responsible health research in Europe.

Funding

The research leading to this article was partially funded by the H2020 RECAP project, grant number 733280 and partially by the IMI BigData@Heart project, grant number 116074. This article reflects the
author’s own views on the subject and not necessarily those of the other partners in these projects.

Conflict of interest statement

Evert-Ben van Veen consults researchers and sometimes patient organisations on regulatory and ethical issues of observational research. He is also a member of the writing group of the BBMRI-ERIC Code of Conduct on health research with data.

Acknowledgements

The author would like to thank the editor, Jan Willem Coebergh, for his editorial comments, Graham Kennett for his help and patience with organising the references and colleagues and clients for their discussions which, although not always in agreement, helped to shape the author’s views.

References


[88] Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the regions on enabling the digital transformation of health and care in the digital single market; empowering citizens and building a healthier society, Brussel 25.4.2018COM. 2018. final.