BRILL
NIJHOFF

EUROPEAN JOURNAL OF HEALTH LAW 25 (2018) 43-55

European Journal of Health Law

brill.com/ejhl

From Privacy to Data Protection in the EU: Implications for Big Data Health Research

Menno Mostert,[a] *Annelien L. Bredenoord,*[a] *Bart van der Sloot*[b] *and Johannes J.M. van Delden*[a]

[a]Department of Medical Humanities, Julius Center for Health Sciences and Primary Care, University Medical Center Utrecht, Utrecht, The Netherlands

[b]Tilburg, Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands

Abstract

The right to privacy has usually been considered as the most prominent fundamental right to protect in data-intensive (Big Data) health research. Within the European Union (EU), however, the right to data protection is gaining relevance as a separate fundamental right that should in particular be protected by data protection law. This paper discusses three differences between these two fundamental rights, which are relevant to data-intensive health research. Firstly, the rights based on the right to data protection are of a less context-sensitive nature and easier to enforce. Secondly, the positive obligation to protect personal data requires a more proactive approach by the EU and its Member States. Finally, it guarantees a more comprehensive system of personal data protection. In conclusion, we argue that a comprehensive system of data protection, including research-specific safeguards, is essential to compensate for the loss of individual control in data-intensive health research.

Keywords

European Union (EU) – data protection – privacy – fundamental rights – Big Data – health research

* M. Mostert, corresponding author, m.mostert-2@umcutrecht.nl.

1 Introduction

Over the last decade, technical possibilities for collecting, re-using and linking data related to individuals have increased tremendously. Moreover, data sharing for health research purposes is increasingly being presented as an ethical and scientific imperative.[1] The effectiveness of certain traditional approaches that govern the use of data in health research is, however, decreasing in the era of Big Data. It has been indicated that a strict 'consent or anonymise approach' neither sufficiently allows for progress in data-intensive health research, nor adequately protects individual rights and interests.[2] In addition, the large scale re-use of data is difficult to reconcile with certain data protection principles, such as purpose limitation and data minimisation.[3] The current debate is about what form laws and information governance — consisting of organisational and technical measures — should take to allow for progress in data-intensive health research while effectively protecting fundamental rights and other morally relevant interests.

This debate usually revolves around the right to respect for private life (hereafter: the right to privacy) as the key fundamental right to protect. Within the EU, however, an independent fundamental right to data protection gradually emerged in addition to the right to privacy.[4] After its separate recognition in the EU Charter of Fundamental Rights, the right to data protection acquired a prominent position in the EU General Data Protection Regulation 2016/679 (GDPR), which will apply from 25 May 2018. Article 1(2) of the GDPR unambiguously affirms that it protects fundamental rights and in particular the right to data protection. This is in contrast to the current EU Data Protection Directive 95/46/EC, which protects in particular the right to privacy with respect to the

1 B.M. Knoppers, J.R. Harris, I. Budin-Ljøsne and E.S. Dove, 'A human rights approach to an international code of conduct for genomic and clinical data sharing', *Human Genetics* 133(7) (2014) 895-903.

2 M. Mostert, A.L. Bredenoord, M.C.I.H. Biesaart and J.J.M. van Delden, 'Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach', *European Journal of Human Genetics* 24(7) (2016) 956-960; Nuffield Council on Bioethics, 'The collection, linking and use of data in biomedical research and health care: ethical issues', February 2015, online at http://nuffieldbioethics.org/project/biological-health-data/, retrieved 20 January 2017.

3 B. Custers and H. Uršič, 'Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection', *International Data Privacy Law*, 6 (1) (2016) 4-15.

4 G.G. Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Dordrecht: Springer, 2014) doi:10.1007/978-3-319-05023-2.

processing of personal data. This change in emphasis is reflected throughout the whole GDPR and therefore also in provisions related to health research. Article 9(2i) of the GDPR is such a provision, which only allows the use of special categories of personal data in health research without consent, when the law provides a derogation that respects the essence of the right to data protection.

It largely remains unclear what this shift from the right to privacy to the right to data protection in the EU means. There is an ongoing debate about the differences between both rights and the rationale for introducing data protection as an independent right.[5] This uncertainty could negatively impact a coherent interpretation and implementation of both fundamental rights and the provisions in the GDPR relevant to data-intensive health research. The aim of this paper is to clarify this matter by discussing whether there are differences between the right to data protection and the right to privacy relevant within the context of data-intensive health research.

2 A Right to Data Protection in the Charter of Fundamental Rights of the EU

In the EU, a fundamental right to data protection sits alongside the right to privacy. The Charter of Fundamental Rights of the EU (the Charter) contains a right to the protection of personal data in Article 8 (the right to data protection), in addition to a right to respect for private life in Article 7 (the right to privacy). In 2009, legally binding force was granted to the Charter in the Lisbon Treaty and the Charter acquired the status of primary EU law. According to its preamble, the Charter "reaffirms" fundamental rights in the EU and makes them "more visible" to strengthen the protection of those rights. Some scholars, however, underline that the Charter did not reaffirm or make the right to data protection more visible, but actually created such a right in addition to the right to privacy.[6] Moreover, the impact of the right to data protection as a separate right is increasingly visible in case law of the Court of Justice of the EU

5 M. Tzanou, 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right', *International Data Privacy Law* 3(2) (2013) 88-99; O. Lynskey, 'Deconstructing data protection: the 'Added-value' of a right to data protection in the EU legal order', *International and Comparative Law Quarterly* 63(3) (2014) 569-597.

6 Fuster, *supra* note 4.

(CJEU).[7] In addition, as mentioned above, Article 1(2) of the GDPR now clearly affirms that the Regulation 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.' In addition, familiar terms, such as "privacy by design" and "privacy impact assessment" have been replaced in the GDPR by "data protection by design" and "data protection impact assessment" (Articles 25 and 35 of the GDPR). Nearly all other references to privacy or the private life have also disappeared in both the legislative text and the recitals.

This way of framing data protection norms in the Charter, the jurisprudence of the CJEU and the GDPR is different from how it has been framed in traditional data protection instruments and case law of the European Court of Human Rights (ECtHR). In the Organisation for Economic Co-operation and Development (OECD) context, national laws on data protection are typically referred to as 'privacy laws'.[8] In Convention 108 of the Council of Europe and EU Directive 95/46/EC, data protection norms are presented as serving in particular the right to privacy. Since the right to data protection, as such, is not included in the European Convention on Human Rights (ECHR), the competence of the ECtHR is limited to personal data processing activities that fall within the scope of Article 8 ECHR, or another right in the ECHR. Personal data processing could fall within the scope of Article 8 ECHR, when the personal data processing engages aspects of the private life. Whether this is the case, depends on the nature of the data, the context in which the data is processed, the way the data is used and the results of the processing.[9]

Furthermore, it should be taken into consideration that the Charter, in itself, is different from traditional human rights instruments, such as the ECHR, in a complex way.[10] The Charter is not a freestanding bill of rights with a universal scope. According to Article 51 of the Charter, it applies to EU institutions and Member States only when they are implementing EU law. Nevertheless, EU and Member State law should, as a minimum, be in accordance with the Charter. Consequently, a provision in EU or Member State law could no longer

7 P. Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation', September 2014, online at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf, retrieved 20 January 2017; J. Kokott and C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law* 3(4) (2013) 222-228.

8 Fuster, *supra* note 4.

9 ECtHR, *Khelili* v. *Switzerland*, App no. 16188/07 (18 October 2011).

10 S. Douglas-Scott. 'The European Union and Human Rights after the Treaty of Lisbon', *Human Rights Law Review* 11(4) (2011) 645-682.

be applicable when it is in conflict with the Charter.[11] An important function of the Charter, therefore, is to guide the implementation and interpretation of EU law, including the GDPR.

3 How Data Protection Differs from Privacy

At first glance, it seems like the right to data protection has dethroned the right to privacy as the key fundamental right to protect, according to Article 1(2) of the GDPR. A closer study however reveals that the reality is more complex, mainly because of the complicated relationship between both rights. In the Charter's explanatory memorandum, it is emphasized that the right to data protection is partially based on the right to privacy.[12] Unfortunately, the memorandum does not adequately explain the justification of a separate introduction of the right to data protection. In addition, there seems to be a large overlap between the scope of both rights.[13] Moreover, both rights serve many of the same objectives.[14] This, combined with the difficulties in defining the right to privacy, makes it difficult to draw a sharp distinction between the two rights. A growing number of legal scholars nevertheless agrees that the right to data protection should not be regarded as an element of, or a mere derivation from, the right to privacy. Moreover, they agree that relevant differences between both rights exist.[15] Below, we identify and discuss three of the differences between the right to data protection and the right to privacy, that we consider most relevant.

3.1 *Individual Rights Decoupled from Privacy*

Firstly, both the scope and the substance of the individual rights guaranteed by the right to data protection differ from those based on the right to privacy. It is the mere processing of personal data that allows data subjects to invoke their

11 CJEU, Case C-399/11, *Melloni*, ECLI:EU:C:2013:107.

12 Convention Praesidium, 'Explanations Relating to the Charter of Fundamental Rights of the European Union, Brussels', 11 October 2000, CHARTE 4473/00, CONVENT 49.

13 Kokott and Sobotta, *supra* note 7; R. Gellert and S. Gutwirth, 'The legal construction of privacy and data protection', *Computer Law & Security Review* 29(5) (2013) 522-530.

14 Lynskey, *supra* note 5.

15 See, among others: Kokott and Sobotta, *supra* note 7; Fuster, *supra* note 4; Hustinx, *supra* note 7; R. Gellert and S. Gutwirth, 'The legal construction of privacy and data protection', *Computer Law & Security Review* 29(5) (2013) 522-530; P. de Hert and S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action', in: S. Gutwirth et al. (eds.), *Reinventing Data Protection?* (New York: Springer, 2009) pp. 3-43.

rights based on the right to data protection. The definitions of 'personal data' and 'processing' are broad. According to Article 4 sub 1 and 2 of the GDPR, these terms cover any operation which is performed on any information relating to a natural person who can be identified, directly or indirectly.[16] Consequently, almost all forms of personal data processing fall under the scope of the right to data protection, regardless of whether the right to privacy is interfered with.[17] In contrast, whether or not the right to privacy is interfered with depends on both the nature and the context of the specific processing.[18] This difference in scope is illustrated by some of the judgements of the CJEU. In the *Rundfunk* judgement, the Court held that "(…) the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life". According to the Court, the recording of personal data, by itself, thus did not fall within the scope of the right to privacy, whereas the Court noted that such a recording falls within the scope of the right to data protection since it constitutes personal data processing.[19] Furthermore, in the *Digital Rights Ireland* case, the CJEU confirmed that the retention of personal data also directly and specifically affects the right to privacy, when the "(…) data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[20] The individual rights based on the right to privacy are, therefore, of a more context-sensitive nature.

In addition to the difference in scope, the substantive protection offered by the right to privacy and the right to data protection also differs. This is illustrated by the confirmation of the ECtHR that the right to privacy does not guarantee a general right of access by the data subject to his own personal data.[21] This is in contrast to the right to data protection, which explicitly guarantees such a right of access in the abstract, irrespective of whether there is an interference with the right to privacy. Some, however, argue that the ECtHR is currently moving towards the introduction of a more general right of access, based on

16 Additionally, see recital 26 of the GDPR.

17 See, among others: Hustinx, *supra* note 7, p. 5; De Hert and Gutwirth, *supra* note 15, p. 9-10.

18 Kokott and Sobotta, *supra* note 7; Lynskey, *supra* note 5.

19 CJEU, Case C-139/01, *Österreichischer Rundfunk and Others*, ECLI:EU:C:2003:294, para. 74 and 64.

20 CJEU, Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014:238.

21 ECtHR, *Gaskin* v. *United Kingdom*, App no. 10454/83 (7 July 1989).

the right to privacy.[22] This growing willingness of the ECtHR to recognise more general rights, based on the right to privacy, makes it increasingly difficult to discern a distinction between the substantive protection offered by both rights. Differences between the substantive protection offered by the right to data protection and the right to privacy do nevertheless remain.[23] These differences may be related to the dissimilar background of the right to data protection, which is also designed to protect non-privacy related interests.

3.2 *A More Positive Approach*

A second difference is that the right to data protection has been designed as a largely *positive obligation* of the EU and its Member States. To fulfil this positive obligation, governments will need to take affirmative measures to protect personal data. In addition, the right to data protection has been designed to regulate both horizontal and vertical relationships. This is in contrast to the right to privacy, which was originally coined as a mere *negative obligation* of public authorities to refrain from arbitrary interference with the private lives of individuals.[24] The ECtHR still considers this negative obligation as the essential object of the right to privacy.[25]

Today, positive obligations related to data-processing activities of private sector entities are nevertheless also inferred from the right to privacy. The ECtHR confirmed that states may be required to adopt measures designed to secure respect for the right to privacy, "even in the sphere of the relations of individuals between themselves".[26] These positive obligations based on the right to privacy do, however, suffer from a number of limitations. One of these limitations is that the concrete positive obligations stemming from the right to privacy are always linked to particular circumstances. This is because what constitutes these positive obligations is predominantly determined by the ECtHR on a case-by-case basis. These cases do not provide a basis for the more general positive obligations as guaranteed by the right to data protection.[27]

The right to data protection therefore complements the positive obligations inferred from the right to privacy with explicit positive obligations that are of

22 Lynskey, *supra* note 5.

23 Hustinx, *supra* note 7; Lynskey, *ibid.*

24 B. van der Sloot, 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 5(3) (2014) 230-244.

25 ECtHR, *Hämäläinen* v. *Finland*, App no. 37359/09 (16 July 2014).

26 ECtHR, *X and Y* v. *the Netherlands*, App no. 8978/80 (26 March 1985).

27 Hustinx, *supra* note 7.

a more abstract nature. Consequently, the somewhat blurred distinction between privacy as an essentially negative obligation and data protection as a largely positive obligation is still relevant.

3.3 *A More Comprehensive and Systematic Approach*

A third difference is that the right to data protection rests on a more comprehensive and systematic approach, one beyond individual rights. Article 8 of the Charter guarantees a comprehensive system of data protection norms and explicitly confirms that the principles of fair and lawful processing, purpose specification and limitation, and the requirement of independent supervision are key elements of this system. In addition, data security — consisting of technical and organisational measures to prevent the accidental loss, alteration or unlawful destruction of the data — was referred to by the CJEU as an essential element of the right to data protection.[28] Other key elements of EU data protection law, such as accountability and data quality requirements, may also implicitly be guaranteed by Article 8(1) of the Charter. Therefore, the right to data protection does not solely rely on individuals who exercise or enforce their rights, but is also based on a set of duties addressed to a broad range of actors involved in personal data processing. Although some of these duties may correlate with individual rights, this is not necessarily the case. An example is that compliance with data protection rules should be subject to control by an independent authority. A similar obligation, just as comprehensive, may not directly result from the case law of the ECtHR based on the right to privacy,[29] especially when it comes to the protection of individuals in horizontal relationships.

The extent to which the right to privacy could embrace similar data protection requirements however remains a complicated matter, since the recognition of data protection norms based on the right to privacy is on a case-by-case basis. Although data security is for instance not regarded as an essential element of the right to privacy,[30] a lack of security measures could result in a violation of the right to privacy, especially when it concerns sensitive health information.[31] Nevertheless, the right to privacy is not considered

28 CJEU, Case C-293/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238.

29 P. de Hert and S. Gutwirth. 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action', in: Gutwirth et al. (eds.), *supra* note 15, pp. 9-10.

30 De Hert and Gutwirth, *supra* note 29.

31 See: *I.* v. *Finland,* App no. 20511/03 (17 July 2008).

to be of a nature to include independent supervision, data security or data quality requirements as its core elements. In other words, the right to privacy does not guarantee a comprehensive system of data protection norms similar to that guaranteed by Article 8 of the Charter.

4 Relevance to Data-intensive Health Research

In the coming years, the EU and its Member States will need to fulfil their positive obligations based on the right to data protection, which have partially been encoded in the GDPR. Moreover, both public authorities and private sector entities will need to interpret the GDPR in accordance with fundamental rights. The increased emphasis on the right to data protection in the GDPR does, however, not necessarily render the right to privacy less relevant, especially in the context of data-intensive health research. After all, health research usually involves the processing of special categories of personal data, such as data concerning health or genetic data, which often engages sensitive aspects of the private life. The right to data protection nevertheless adds an important layer of protection, as we discuss below.

4.1 *The Impact of Individual Rights*

The individual rights rooted in Article 8 of the Charter could have a significant impact on data-intensive health research. Even though the right to data protection guarantees a system of data protection beyond individual rights, the individual rights of data subjects are still an essential element of this system. This may be why the allowed derogations from some of the individual rights in the GDPR are of a limited nature, especially when these rights are guaranteed by Article 8 of the Charter. Derogations from the right of access and the right to rectification (Article 8(2) of the Charter) for scientific research purposes may only be provided by law 'in so far as the individual rights would render impossible or seriously impair the achievement of the specific purposes(..)' (Article 89(2) in conjunction with Articles 15 and 16 of the GDPR). Moreover, derogations or exceptions from the right to information are not allowed at all when personal data are collected from the data subject himself (Article 13 of the GDPR). This right to information of the data subject is part of what constitutes "fair" processing, as referred to in Article 8(2) of the Charter.

A negative impact of these individual rights on data-intensive health research may nevertheless be reduced by taking them into account throughout the process of engineering information systems and shaping information

governance. Those responsible for Big Data infrastructures and projects know beforehand which rights data subjects could invoke. This is due to the decoupling of the scope of individual rights of data subjects from an interference with the right to privacy, which results in more legal certainty. Implementing technical and organisation measures to ensure that data subjects can invoke their rights and that data-protection principles are implemented is not a mere opportunity for data controllers. It also is a legal obligation laid down in Article 25 of the GDPR under the title "Data protection by design".

4.2 *Safeguards beyond Individual Rights and Consent*

The more positive and comprehensive approach required by the right to data protection is of great importance to allow progress in data-intensive health research in a responsible way. The key strength of the system of data protection is that it does not merely rely on strengthening individual rights or consent requirements to protect and balance relevant rights and interests.

After all, individuals are often no longer able to make meaningful decisions about the use of their personal data, as a consequence of the rapidly increasing scale and complexity of data-intensive health research.[32] Although efforts are made to enhance the exercise of individual control in health research by the use of online portals and engaging individuals as active participants,[33] it must be recognised that individuals can only selectively choose to be engaged. 'Broad consent' models, as referred to in Recital 33 of the GDPR, do recognise this to some extent by inviting people to agree to a broad range of future data use in research. This however inevitably leads to a trade-off between obtaining consent in a simple and practicable way, and providing individuals with sufficient information and control. Moreover, strengthening individual rights and consent requirements does not necessarily, in itself, reduce the risks to which individuals are exposed. What is more, merely relying upon consent and individual rights would not only result in an ineffective protection of individuals and their interests, it could also disproportionately hamper progress in data-intensive health research.[34] This is because it is often impracticable or impossible to allow individuals to exercise meaningful control over the use of their personal data in data-intensive health research.

---

32 Mostert, *supra* note 2.

33 J. Kaye et al. 'Dynamic consent: a patient interface for twenty-first century research networks', *European Journal of Human Genetics* 23 (2015) 141-146.

34 See: *supra* notes 2 and 3; C.T. Di Lorio, F. Carinci and J. Oderkirk, 'Health research and systems' governance are at risk: should the right to data protection override health?', *Journal of Medical Ethics* 40(7) (2014) 488-492.

The EU legislative bodies seem to have taken these considerations into account, not only by allowing derogations in favour of scientific research from consent requirements and some of the individual rights,[35] but also by requiring that such derogations should be subject to appropriate safeguards in accordance with the GDPR and the rights and freedoms of the data subject.[36] In addition, when derogating from the obligation to obtain consent for the use of special categories of personal data for scientific research purposes, Article 9(2i) of the GDPR explicitly underlines the importance of respecting the essence of the right to data protection and providing for suitable and specific safeguards by law. By means of these derogations, the EU aims to facilitate scientific research, as long as the processing of personal data is subject to appropriate conditions and safeguards set out in EU or Member State law.[37] An important part of these derogations and safeguards, however, still need to be implemented in Member State law.[38] It thus becomes clear that respecting the right to data protection, while sufficiently allowing for progress in data-intensive health research, requires proactive legislators. When the EU and its Member States take this positive obligation serious, the GDPR could indeed be regarded as a step forward for data protection and health research.[39]

By way of contrast, the effectiveness of data protection law in regulating data-intensive health research has also been criticised. Some scholars have argued that the term personal data is poorly defined and have raised questions about what data or communications should be protected by law.[40] Others have suggested that the limits of the law should be recognised and the strengths of soft law options such as ethical guidance or professional codes should be more

35 For an overview of these derogations see: The Wellcome Trust, 'Analysis: Research and the General Data Protection Regulation', July 2016, online at https://wellcome.ac.uk/sites/default/files/new-data-protection-regulation-key-clauses-wellcome-jul16.pdf, retrieved 20 January 2017.

36 See: Article 89(1) of the GDPR.

37 See: recital 157 of the GDPR.

38 The Wellcome Trust, 'Implementing the General Data Protection Regulation [2016/679] to maintain a competitive environment for research in Europe', September 2016, retrieved 20 January 2017 http://www.scienceeurope.org/wp-content/uploads/2016/10/EU-GDPR-implementation-Sep-2016.pdf.

39 E.S. Dove, B. Thompson, B.M. Knoppers, 'A step forward for data protection and biomedical research', *The Lancet* 387(10026) (2016) 1374-1375.

40 O. O'Neill, 'Can Data Protection Secure Personal Privacy?', in: T.S. Kaan, C.W. Ho (eds.), *Genetic Privacy* (London: Imperial College Press, 2013) pp. 25-40.

appreciated.[41] In their view, data protection law should provide for sufficiently open norms to allow for soft law instruments, such as the international governance frameworks that are currently being developed.[42] The GDPR seems to meet this requirement, since Article 89(1) of the GDPR does not impose any strict safeguards on personal data processing for scientific research purposes. According to Article 89(1) of the GDPR, appropriate safeguards should "ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation". This obligation is weakened by adding that measures of data minimisation, which may include pseudonymisation, only need to be taken when the research purposes can be fulfilled in that manner. Moreover, Article 5(1c) of the GDPR already requires similar measures of data minimisation as an overarching safeguard.

Nonetheless, Article 89(1) of the GDPR does play a pivotal role in the protection of personal data when derogations from consent or individual rights are provided in favour of health research. In addition, as long as the data processing is in accordance with this provision, the re-use of personal data for scientific research purposes is not considered to be incompatible with the principles of purpose limitation and data minimisation (Article 5(1b) of the GDPR). It is therefore striking that Article 89(1) of the GDPR only provides very limited points of departure for what specific safeguards should be in place in a research context.

5 Conclusion

Although the rights to privacy and data protection are closely related, they should not be considered as identical. The right to data protection adds a crucial layer of protection beyond essentially negative obligations, individual rights based on the right to privacy, and consent requirements. It aims to complement the right to privacy by positively guaranteeing a more comprehensive and harmonised system of data protection norms, which are relatively easy to enforce and comply with.

Within the context of data-intensive health research, such a comprehensive system of data protection should be considered to serve two functions in

41 G.T. Laurie and N. Sethi, 'Delivering proportionate governance in the era of eHealth: Making linkage and privacy work together', *Medical Law International* 13(2-3) (2013) 168-204.

42 B.M. Knoppers, 'Framework for responsible sharing of genomic and health-related data', *The Hugo Journal* 8 (2014) 3.

particular. Firstly, the aim is to provide effective *overarching safeguards* that secure the rights and interests of individuals, irrespective of whether the personal data processing is grounded on consent or any other legal basis. After all, merely adhering to the principle of lawfulness is never sufficient to respect the right to data protection. Secondly, such a system of data protection arranges for *specific safeguards* when it is necessary and proportional to derogate from consent requirements or certain individual rights. These specific safeguards are also essential to allow for the re-use of personal data in data-intensive health research, without taking heed of the principle of purpose limitation. The overarching safeguards should, amongst other things, include requirements of accountability subject to independent oversight, transparency towards data subjects and the public, ensure that data subjects can invoke their rights and data security. The issue of which specific safeguards should be provided for by law with regard to data-intensive health research remains unclear and deserves further study. After all, these specific safeguards should compensate for the loss of individual control as a result of the exceptions from individual rights and consent requirements for health research purposes.

At the same time, the limits of data protection law should be recognised. Relying on the distinction between personal and non-personal data to protect privacy and other relevant rights and interests might prove to be inadequate. In addition, inflexible or static data protection laws could hamper the development of suitable information governance frameworks on the national or international scale, in which the myriad of ethical, legal, social and professional norms need to be reconciled.