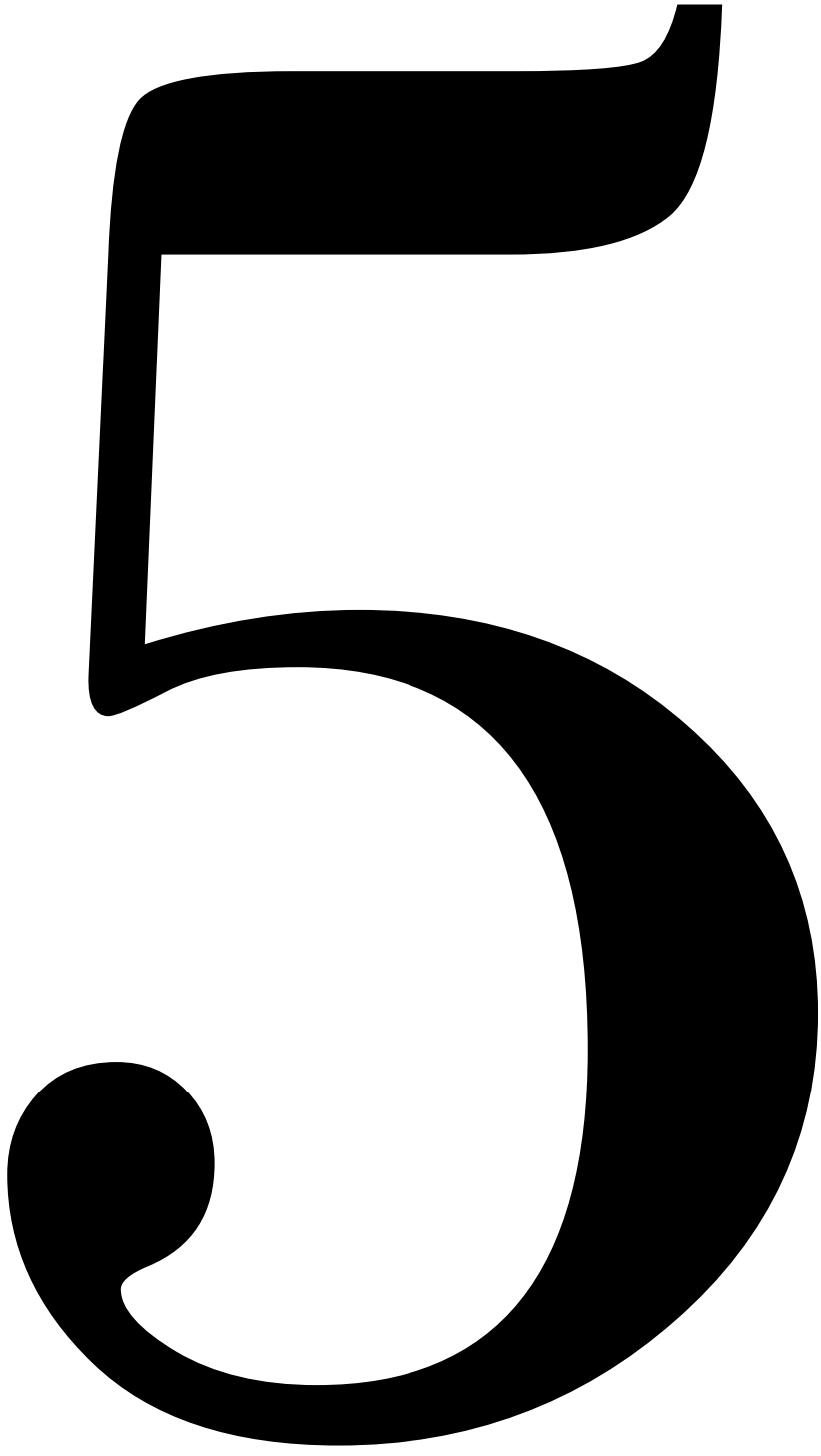
A fair balance: health data protection and the promotion of health data use for clinical and research purposes

Kist, I.R.



Proposal for a new data regime in the UK: an avenue to be explored by the EU

5. Proposal for a new data regime in the UK: an avenue to be explored by the EU[371]

This chapter answers sub-question 4 that reads as follows:

In what way do the developments in the United Kingdom serve as an avenue to be explored in the European Union with regard to the further use of health data for secondary health research?

[371] I.R. Kist, Proposal for a new data regime in the UK: an avenue to be explored by the EU, *European Data Protection Law Review* 8 (2022) (2), 295-301. DOI https://doi.org/10.21552/edpl/2022/2/18.

5.1. Introduction

When the UK formally left the European Union on 31 December 2020 at 11 PM after a transition period of one year, the GDPR was retained in domestic UK law as the UK GDPR. However, the UK is at liberty to keep the framework under review. The UK GDPR applies alongside an amended version of the Data Protection Act (DPA) 2018.[372] Thus, the main principles, rights and obligations have remained the same even after the beginning of 2021. At present, however, the so-called retained EU law, which includes the UK GDPR, may undergo significant amendment. In its document *Data: a new direction*, published by the Department for Digital, Culture, Media & Sport (DCMS) on 10 September 2021, the UK set off on a new and different path from the EU.[373] The primary aim is to reduce regulatory burdens and to lessen the resources required for compliance. A parallel development has been the UK's National Data Strategy, announced in June 2018 by the Secretary of State for the Department for Digital, Culture, Media & Sport (DCMS), which aims at unlocking the power of data across the government and wider economy. This strategy also aims at building citizen trust in the data ecosystem and at supporting the UK towards a world-leading data economy. Furthermore, on 31 January 2022, the UK government announced the 'Brexit Freedoms Bill'.[374] The Bill was included in the Queen's Speech in May 2022 and received Royal Assent on 29 June 2023 following agreement of both Houses in Parliament.[375] Two other bills were also announced in the Queen's Speech, i.e., the Data Reform Bill and the Bill of Rights.[376] The legislative developments in the UK could have implications for the free flow of data from the EU to the UK.[377]

[372] The UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. https://www.legislation.gov.uk/ukdsi/2019/9780111177594/pdfs/ukdsi_9780111177594_en.pdf. Data Protection Act, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Accessed 6 June 2022.

[373] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf. Accessed 6 June 2022. Also, House of Commons, European Scrutiny Committee, Oral evidence: Retained EU Law: Where next? HC 1113, 9 February 2022. And UK Government, *National Data Strategy*, updated 9 December 2020, Department for Digital, Culture, Media & Sport, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy. Accessed 6 June 2022.

[374] The Brexit Freedoms Bill is part of the European Union (Withdrawal Agreement) Act 2020, https://www.legislation.gov.uk/ukpga/2020/1/contents. Accessed 6 June 2022.

[375] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf. Accessed 6 June 2022. Also, https://www.parliament.uk/business/news/2023/february-2023/lords-debates-retained-eu-law-revocation-and-reform-bill/. Accessed 22 January 2024.

[376] In the meantime, the UK government introduced the Data Protection & Digital Information Bill (No. 2) on 8 March 2023. This Bill withdrew the Data Protection the Data Protection & Digital Information Bill that was introduced in June 2022. https://bills.parliament.uk/bills/3430/. Accessed 22 January 2024. The Bill of Rights was withdrawn on 27 June 2023. https://bills.parliament.uk/bills/3227. Accessed 22 January 2024.

[377] Responses to the consultation: UK Government, Data: a new direction, https://www.gov.uk/government/consultations/data-a-new-direction. Accessed 7 June 2022.

This chapter addresses the proposed changes to data protection law in the UK and the UK National Data Strategy.[378] It focuses particularly on the proposed changes for scientific research. Thus, this analysis does not include all amendments as proposed. The chapter starts with an outline of the limitations and deficiencies to scientific research in the UK GDPR (section 5.2). Next, it elaborates on the proposed amendment (section 5.3). An argument will be made that the amendment is an avenue to be explored by the EU with its potential benefits for scientific research. The chapter then elaborates on potential risks to the data protection landscape and the data subject. Subsequently, the implementation of the GDPR in the Netherlands with regard to scientific research will be used as an example (section 5.4). The latest EU developments will be briefly referred to as well, before ending with a conclusion (section 5.5).

5.2. UK GDPR – Limitations and deficiencies of scientific research

5.2.1. Barriers to responsible innovation and data flows

The interpretation of the law, as well as general definitions in the law without explanatory case law (yet) or regulatory guidance, have resulted in the full capacity of data sharing not always being used. Furthermore, the elaborations on the lawful basis for the re-use or secondary use of research data have resulted in an over-reliance on asking consent from individuals. Seeking (additional) consent may hamper the efficiency of research and may place a burden on the individual, i.e., the data subject. Additionally, increasing technological innovations, including the use of artificial intelligence and the vast amount of data require clearance about this use with consistent rules. Moreover, the UK GDPR includes both the recitals and the articles of the law. However, some recitals related to scientific research have not been adopted in the plain text of the UK GDPR. Hence, the relevant clauses on international data transfers, in particular as regards adequacy regulations (article 45 UK GDPR), appropriate safeguards (article 46 UK GDPR), and derogations (article 49 UK GDPR), place restrictions on these transfers, and, consequently, on international, multi-center research.[379]

5.2.2. Barriers to scientific research

In addition to these barriers to responsible innovation and data flows, there are specific barriers to scientific research. The recitals and provisions on scientific research are dispersed across the UK GDPR and the Data Protection Act 2018, whereas the content of the recitals is not always incorporated into the plain text of the UK GDPR. As a result, researchers are unaware of which legal obligations they must fulfill and whether exemptions to the general rules apply to their research. Guidance by the Information Commissioner's Office (ICO) alone will not suffice to solve the uncertainty and

[378] Policy paper, updated 9 December 2020, https://www.gov.uk/government/publications/uk-national-data-strategy. Accessed 6 June 2022.
[379] P. Breitbarth, A risk-based approach to international data transfers, *European Data Protection Law Review* 4 (2021), 540-549.

ambiguity in the law.[380] Thus, legal reform is necessary in this respect. Furthermore, an additional, separate lawful basis for research, or clarity about the use of the lawful bases of the public interest or legitimate interests, may prove useful to organizations that undertake scientific research.

Additionally, the further processing of personal data, i.e., re-using the data for another research purpose, has been subject to lively debate.[381] Article 5 (1) (b) UK GDPR states that further processing of personal data for scientific or historical research purposes shall not be considered incompatible with the initial purposes, provided that the necessary safeguards are in place.[382] Moreover, although the broader conditions for determining compatibility of the purposes for further processing are enshrined in article 6 (4) UK GDPR, it cannot be deduced from this clause when personal data may be re-used for another purpose than that for which they were collected in the first place. Secondly, it is unclear whether personal data may be re-used by a different controller than the original controller that collected the data in the first place, and whether this collection by the second controller constitutes further processing. Thirdly, the question arises whether the further processing is subject to a new determination of the lawful basis, both in cases where the further processing is either compatible or incompatible with the original purpose as referred to in article 5 (1) (b) together with article 6 (4) UK GDPR.

There is lively debate surrounding the concept of broad consent.[383] While it has been acknowledged that an individual gives his consent for broad(-er) areas of scientific research, the scope of consent is subject to discussion. A second issue concerns the reconciliation of the concept of broad consent with the elements of valid consent as defined in article 4 (11) UK GDPR, i.e., that the consent must be freely given, specific, fully informed, and unambiguous. The question arises what constitutes 'broad' in broad consent. Furthermore, the lawful bases of the public interest and legitimate interests have yet to be fully explored as regards scientific research (as well as other domains where personal data are processed).

Artificial intelligence (AI) and machine learning have become important components of scientific research.[384] The use of data in this field requires that specific attention be

[380] https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/. Accessed 6 June 2022.
[381] European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, 6 January 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf. Accessed 6 June 2022.
[382] Recital 50 GDPR. The GDPR is saved into UK law through section 3 of the European Union (Withdrawal) Act 2018 ("EUWA"). This includes the recitals to the GDPR.
[383] E. Gefenas et al., Controversies between regulations of research ethics and protection of personal data: informed consent at a cross-road, *Medicine, Health Care and Philosophy* (2022) (25), 23-30 https://doi.org/10.1007/s11019-021-10060-1.
[384] UK Government, *National AI Strategy*, https://www.gov.uk/government/publications/national-ai-strategy, published on 22 September 2021. Accessed 7 June 2022.

paid to its collection, curation, storage, and removal. The UK GDPR and the Data Protection Act 2018 are technology-neutral, although the UK GDPR distinguishes between the use of data for research and non-research purposes. The fact that the data protection framework does not distinguish between the different uses of data within an AI process may result in uncertainty about the lawful basis and the purpose(s) of data processing. Furthermore, a distinction is necessary in the various phases of an AI process, from development to deployment. Additionally, clarification is required about the circumstances surrounding when personal data will be regarded as anonymous. Since the UK GDPR only applies to personal data that can be re-identified, directly or indirectly, this determination is important to delineate the applicable law to data processing.

5.2.3. Rule-based regulatory compliance

Although one of the main principles as set out in article 5 UK GDPR concerns the accountability of the controller, a rule-based system of regulatory compliance has been established. This system, together with a specific number of requirements that organizations must fulfill to demonstrate compliance, places an unnecessary burden on organizations as well as data subjects, since energy is devoted to demonstrating compliance rather than to developing better practices and, thus, protecting the personal data and data subject's rights. For instance, article 30 UK GDPR requires a record of processing activities by the organization and article 35 UK GDPR requires a Data Protection Impact Assessment (DPIA) in case of processing personal data which is likely to result in a high risk to individuals. Furthermore, article 36 UK GDPR requires prior consultation in case an organization has identified a high risk for data processing that cannot be mitigated, and articles 37 to 39 UK GDPR require the appointment of a data protection officer. Furthermore, articles 33 and 34 UK GDPR set out the rules for reporting a data breach. Only those breaches where a risk to individuals is not material are exempted from notification. However, the scope of a non-material breach remains unclear. All clauses referred to above fall within a system of rule-based regulatory compliance, rather than a risk-based approach.

5.3. Proposal for a UK GDPR amendment

5.3.1. Reducing barriers to responsible innovation and data flows

The UK government realizes that AI technology, big data research, and machine learning are of prime importance to innovations. At the same time, these innovations require a robust approach to data protection. The government proposes a further dialogue on the scope of transparency and fairness as regards data processing to these ends, where a balance can be found among these innovations as well as in responsible and trustworthy AI developments. For instance, data processing may be necessary in order to detect biases and to mitigate risks. If this data processing is subject to

the explicit consent from the data subjects, the AI application may not represent a complete data population. Thus, the AI application itself may become biased. The government proposes that this processing constitutes a legitimate interest pursuant to article 6 (1) (f) UK GDPR, so that the AI system can monitor, detect, and correct biases. The government proposes particular attention to be drawn to the use of sensitive data in this respect, i.e., regarding the purpose for which the data are collected and the appropriate safeguards that are in place to mitigate the risks of secondary use. The government aims at furthering public trust in data collection for innovation.

Thus, the government proposes further clarity on data minimization, such as pseudonymization, and a clear distinction between anonymized and pseudonymized data. Whereas pseudonymized data fall within the scope of the UK GDPR, anonymized data do not. The government proposes a relative approach in this respect.[385] Furthermore, the government proposes a risk-based approach to adequacy regulations in international data flows. Additionally, in case an adequacy decision has not been given, the government proposes alternative transfer mechanisms where the data subject's rights are respected. The government intends to facilitate more detailed, practical support in determining and addressing risks with regard to these transfers. One of these alternative transfer mechanisms includes the certification scheme and the government proposes a common, inter-operable approach based on the principles of accountability. Lastly, the government proposes that the derogations enunciated in article 49 UK GDPR be invoked in case of repetitive data transfers as well.

5.3.2. Reducing barriers to scientific research

The UK government proposes that research-specific provisions be consolidated and concentrated to clarify the large amount of provisions and their correlations. In this respect, a definition of scientific research is desired in the provisions of the UK GDPR, rather than an explanation in recital 159 UK GDPR. As regards the lawful basis or bases of scientific research, the government considers the following. First, the lawful basis of the public interest (article 6 (1) (e) UK GDPR) could be another lawful basis to be relied upon by university research projects, in addition to the lawful basis of consent. Second, a separate lawful basis for scientific research could reduce the burden for organizations seeking a proper lawful basis for their research, if the safeguards as enshrined in article 89 (1) UK GDPR be adhered to at all times.

Next, as regards the re-use or further processing of personal data for a purpose other than the original collection of data, the government proposes to clarify the concept of (broad) consent, as well as offer a clarification on article 5 (1) (b) of the UK GDPR

[385] Judgment of the Court (Second Chamber) of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland. Case C-582/14. ECLI:EU:C:2016:779.

on the compatibility of the further use of data for research purposes. In concrete terms, the government proposes that the further use of data for scientific research is always compatible with the original purpose, and that it is always lawful pursuant to article 6 (1) of the UK GDPR. In this respect, the government reiterates the necessity of transparency to the data subjects whose data are used, and the technical and organizational measures to be taken by the controller in order to guarantee the data subject's rights and freedoms.

As regards the re-use of data for a purpose different from that for which they were collected, the government proposes that the further processing for an incompatible purpose may be allowed when the processing safeguards an important public interest. To this end, the government proposes a clarification on article 6 (4) of the UK GDPR. Similarly, the government proposes clarity on the further processing by a different controller. At present, controllers are uncertain whether they can do so lawfully, while ensuring fairness and transparency. Additionally, a similar uncertainty exists regarding the lawful basis of the further processing. For example, if the new purposes for processing are incompatible with the original purpose, controllers question whether the further processing can be permitted. The government proposes that the further processing indeed be permitted, whether it be incompatible or compatible with the original purpose, if the further processing be based on a law that safeguards an important public interest.

With respect to the lawful bases of data processing, the government concludes that the lack of clarity and certainty regarding the use of the different lawful bases in article 6 UK GDPR may have resulted in an over-reliance on the lawful basis of consent pursuant to article 6 (1) (a) UK GDPR, and far less reliance on the lawful basis of the legitimate interests pursuant to article 6 (1) (f) UK GDPR. To this end, the government refers to the Data Protection Act 2018, which includes an exhaustive list of legitimate interests relating to which consent from the data subjects need not be asked.

5.3.3. Risk-based regulatory compliance

The government proposes a more flexible and risk-based accountability framework, based on privacy management programs implemented by the organizations themselves and on the scope of the data processing activities. Furthermore, the government proposes that specific legal requirements in the current UK GDPR be removed, as referred to in sections 5.3.1 and 5.3.2 above. Examples are the register of data processing activities, the requirement of a data protection officer, the data protection impact assessment, and the prior consultation with the Information Commissioner's Office. To this end, the government enhances tailor-made approaches by the organizations

in their specific circumstances with the common aim of identifying, mitigating, and minimizing privacy risks of data processing. As regards data breaches, the government proposes that only those data breaches be reported that are likely to result in a risk to the rights and freedoms of the data subject. In short, the government proposes a proactive approach from the organizations to demonstrate accountability and transparency while the burden of demonstrating compliance is reduced at the same time.

5.3.4. Analysis: the UK's changes to the retained EU law

The foregoing seems to suggest that the proposed reforms benefit data sharing in the pursuit of scientific research.[386] However, in my view a few points merit consideration. First, if the UK government significantly alters, and partly removes, retained EU law through the Brexit Freedoms Bill and the Data Reform Bill, the question arises how the new UK legislation will relate to the GDPR. A deviation from the EU's data protection regime may have an impact on the UK to maintain EU adequacy. I applaud the desire for innovation, scientific research as well as clarity in the data protection legal landscape and, hence, data sharing. At the same time, these changes might erode the UK's data protection regime overall and the data subject's rights in particular. The Information Commissioner's Office, in its response to the DCMS Consultation,[387] argued that "innovation is enabled, not threatened, by high data protection standards."[388] Furthermore, new legislation could result in a further divergence between the UK and EU GDPR. The free flow of data, both within the EU and between the EU and the UK, serves as an engine for economic growth. Both the EU and the UK have an interest in the free flow of data and, therefore, the UK's adequacy remains pivotal. A balance must be found between the data protection landscape vis-à-vis the free flow of data to further scientific research and innovations.

5.4. Potential benefits of the UK GDPR amendment for scientific research: the example of the Netherlands

I would argue that the holy grail of the UK GDPR amendment can be found in the risk-based approach as a guiding principle throughout the proposal, together with the attention given to accountability, transparency, and trust. This approach would also benefit scientific research in the Netherlands, a data-intensive economy where both national and international collaboration are prerequisites for enhancing scientific research. Thus, the proposed changes referred to above with regard to international data flows, a clarification on pseudonymization and anonymization, a broader use of

[386] UK Government, The benefits of Brexit, https://www.gov.uk/government/publications/the-benefits-of-brexit. Accessed 7 June 2022.
[387] Department for Digital, Culture, Media and Sport.
[388] Information Commissioner's Office, Response to DCMS consultation "Data: a new direction", 06 October 2021. https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf. Accessed 7 June 2022.

other lawful bases in addition to the lawful basis of consent, a solid AI strategy, and risk-based regulatory compliance, will prove useful for the organizations that process personal data as well as for the data subjects whose data must be protected.

The UAVG is policy-neutral.[389] The provisions pursuant to the previous Dutch Data Protection Act (*Wet bescherming persoonsgegevens,* hereinafter: Wbp)[390] have been incorporated into the new legislation, as far as they are compatible with the GDPR. The UAVG is currently under revision.[391] The GDPR is technology-neutral, while new developments progress rapidly. For instance, the COVID-19 pandemic has shown the necessity once again for international, multi-center data sharing to foster scientific research and to combat life-threatening diseases. A new light shed on the GDPR and the UAVG may increase efficiency in data sharing, whereas the data subjects and their data are equally protected. Furthermore, risk-based regulatory compliance will yield similar results in the Netherlands, as described above in the UK. It will enhance efficacy and efficiency in organizations that process personal data.

In the meantime, new developments are taking place in Europe. The European strategy for data includes new European legislation. On 25 November 2020, the European Commission published a proposal for a regulation on data governance.[392] The Data Governance Act (DGA) entered into force on 23 June 2022 and became fully applicable in the EU on 24 September 2023, following a transitional period of 15 months. The EU aims to create a single European market for data to guarantee the free flow, share, and re-use for the benefit of individuals, researchers, corporate entities, and public administrations. The Data Governance Act creates the processes and structures to facilitate data use.

The Data Act also clarifies who can create value from data and under what conditions.[393] The Data Act entered into force on 11 January 2024.[394] On 3 May 2022, the European Commission presented a proposal for a regulation on the European

[389] Enacted on 16 May 2018, https://wetten.overheid.nl/BWBR0040940/2021-07-01. On this, cf. Paul Breitbarth, GDPR Implementation Series Netherlands: The UAVG (2018) 4(3) EDPL 360-365.
[390] Enacted on 6 July 2000, https://wetten.overheid.nl/BWBR0011468/2018-05-01. Replaced by the GDPR on 25 May 2018.
[391] Tweede Kamer (Lower House of Dutch Parliament), vergaderjaar (year of session) 2019–2020, 32 761, nr. 164. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z10112&did=2020D21909. Accessed 6 June 2022.
[392] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act, DGA), COM/2020/767 Final, 25 November 2020.
[393] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM (2022) 68 Final Brussels, 23 February 2022.
[394] https://digital-strategy.ec.europa.eu/en/news/european-data-act-enters-force-putting-place-new-rules-fair-and-innovative-data-economy. Accessed 22 January 2024.

Health Data Space.[395] The EHDS is one of nine European data spaces identified in the European Commission's 2020 European Strategy for Data. It builds on the Data Governance Act and the Data Act. These acts are horizontal in nature, while the EHDS Regulation includes specific sectoral measures in the area of health, both as regards the use of data for health care (primary use) and the re-use of health data (secondary use). These deliverables aim to regulate both the free flow and use of data and to expand the rights of citizens to access and portability of health data. In that view, the EU developments are promising. Yet, the proposals do not address specific questions about the use of data for scientific research. The European Commission raised these questions at an earlier stage.[396] The UK government addresses these particular questions in more detail.

5.5. Conclusion

This chapter answered sub-question 4 that reads as follows:

> *In what way do the developments in the United Kingdom serve as an avenue to be explored in the European Union with regard to the further use of health data for secondary health research?*

The proposals by the UK government are a good starting point for a further elaboration in the EU in general and the Netherlands in particular for the following four reasons. Firstly, the risk-based approach has been included throughout the proposal, together with the attention drawn to accountability, transparency and trust granted by the data controller as regards data sharing.

Secondly, the lawful basis of the public interest (article 6 (1) (e) UK GDPR) could be another lawful basis to be relied upon by university research projects. Additionally, a separate lawful basis for scientific research, together with the safeguards of article 89 (1) UK GDPR, could reduce the burden for organizations seeking a proper lawful basis for their research. The use of the lawful basis of the public interest or a separate legal ground for scientific research may solve the predominant focus on the legal ground of consent. As regards the lawful basis of consent, the concept of (broad) consent is further clarified. Furthermore, the further use of data for scientific research

[395] European Health Data Space Regulation, Proposal for a regulation - The European Health Data Space (europa.eu). Accessed 9 May 2022. https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_en#governance-of-the-european-health-data-space. Accessed 13 April 2022. Legislative train schedule on https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-european-health-data-space. Accessed 13 April 2022. A Commission's presentation for the European Public Service Union of 3 February 2022: https://www.epsu.org/sites/default/files/article/files/EHDS%20presentation.pdf. Accessed 13 April 2022. Hereinafter EHDS.

[396] European Data Protection Board, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Adopted on 2 February 2021, https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf. Accessed 7 April 2022.

is considered compatible with the original purpose. To this end, transparency to the data subjects and measures taken by the controller are of importance.

Thirdly, the further processing for an incompatible purpose could be allowed if the processing safeguards an important public interest. Article 6 (4) UK GDPR merits further clarification to this end. Thus, the further processing may be permitted, whether it be incompatible or compatible with the original purpose if the further processing were based on a law that safeguards an important public interest. The UK government concludes that the lack of clarity and certainty regarding the use of the different lawful bases in article 6 UK GDPR may have resulted in an over-reliance on the lawful basis of consent pursuant to article 6 (1) (a) UK GDPR, and far less reliance on the lawful basis of the legitimate interests pursuant to article 6 (1) (f) UK GDPR.

Fourthly, a risk-based approach to international data transfers will facilitate international data sharing. Adequacy decisions are one way to enable international data sharing. Alternative transfer mechanisms where the data subject's rights are respected could be of value as well. One of these alternative transfer mechanisms includes a certification scheme, based on the principle of accountability on behalf of the data controller. Furthermore, the derogations enunciated in article 49 UK GDPR should be invoked in case of repetitive data transfers as well.

However, the proposals also leave room for further discussion. For example, the proposals refer to the processing when "it safeguards an important public interest." Further elaboration on what constitutes "an important public interest" is desirable. Similarly, the proposal refers to processing "in the substantial public interest" in the case of sensitive personal data. A complete overview of those data that may be processed "in the substantial public interest" has not yet been finalized.

Secondly, the proposals for international transfer mechanisms, other than those based on an adequacy decision raise further questions. For example, one of the approaches includes the empowerment of organizations to create their own transfer mechanism. The UK follows the data protection regime of New Zealand in this respect, and it raises questions about the minimum criteria to be met as well as the boundaries to this flexibility. One must bear in mind, however, that new approaches may have an impact on the UK's adequacy status itself. A further analysis on the free flow of data on the one hand, and safeguarding the interests of the data subjects on the other, is needed.

Thirdly, as regards the lawful bases for processing, the UK government proposes that the lawful bases of the public interest and legitimate interests be scrutinized in case

of the (further) use of personal data for scientific research. At the same time, the government proposes that a separate, new lawful basis for scientific research, together with the safeguards of article 89 UK GDPR, be examined. The European landscape, with its wide variety of implementation legislation of the GDPR and, likewise, the use of lawful bases for the further use of personal data for scientific research, may not be served with yet another lawful basis. Rather, a more flexible, risk-based approach to the use of the existing lawful bases may yield similar results. Nevertheless, recent developments in both the UK, the European Union and the Netherlands point towards the use of other lawful bases for scientific research. The developments of the EHDS and Wzl underpin this.

Lastly, risk-based regulatory compliance not only requires a different approach from the organizations that process data, but also from the data protection authorities that monitor compliance. Furthermore, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) play an important role in this respect as well. Thus, a different approach in the UK requires another role and, therefore, reform of the Information Commissioner's Office. A different approach to regulatory compliance in Europe requires another role and reform of the national data protection authorities in the first place. Furthermore, a new design of both the roles of the EDPB and EDPS may be required as well. Nevertheless, the UK's National Data Strategy on scientific research certainly is an avenue to be explored by the EU since it addresses the challenges both the EU and UK currently face. In that sense, one can look forward to the developments in the UK as well as those on the mainland to see whether they reach the welcome goals of furthering scientific research and protecting the data subject.