European Digital Media Observatory

Institute for Data, Democracy & Politics
THE GEORGE WASHINGTON UNIVERSITY

Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access

31 May 2022

This project has received funding from the European Union under Contract number: LC-01464044.

George Washington University's Institute for Data, Democracy & Politics was established by a grant from the John S. & James L. Foundation.

Note from the Working Group Chair

This report summarizes the work and shares the findings of a cross-sector, multi-stakeholder Working Group established by the European Digital Media Observatory (EDMO) in May 2021 to begin drafting a Code of Conduct under Article 40 of the General Data Protection Regulation (GDPR) on platform-to-researcher data access. The Working Group's twelve members—drawn from academia, civil society, and industry—met regularly over the last year to consider the legal, ethical, technical, and scientific possibilities for facilitating data access.

Academic and civil society researchers have been calling for greater access to digital platform data—data that would allow greater insights into the impacts these platforms have on individuals, social groups, and our societies as a whole—for some time. Concerns about the spread of mis- and disinformation, political polarization, discriminatory advertising, among many others, require greater scrutiny by independent researchers who, in turn, communicate their findings to the public and policymakers. But without greater access to platform data, in many instances, such scrutiny remains difficult, if not impossible.

At the same time, digital platforms have raised important concerns about the ethical and privacy implications of sharing platform data with external researchers. The data of greatest interest to researchers often represent personal, and sometimes sensitive, information about the beliefs, attitudes, and behaviors of platform users.

With a mind to protecting this information—and, thereby, the fundamental rights of platform users—the GDPR places limits on the ways in which both platforms and researchers can process personal data. Yet, the GDPR does not *prohibit* platform-to-researcher data access. To the contrary, it recognizes the importance of research for our societies, and therefore introduces exceptions to strict limitations on processing personal data for research purposes. In some areas, the GDPR's limitations on data processing activities are relatively clear. In others, neither platforms nor researchers have had a clear view of the implications of the GDPR for their work. Moreover, the GDPR itself does not lay out specific guidance on *how* platform-to-researcher data access might legally be achieved.

Thus, the members of the EDMO Working Group set out to begin developing a Code of Conduct that would provide such guidance. This report provides information about the Working Group's background and motivations, its composition and procedures, as well as some of the key issues that its members discussed as they examined how to responsibly facilitate data access in a way that is compliant with the GDPR.

The report also provides draft language intended to lay the groundwork for a Code of Conduct on Platform-to-Researcher Data Access under Article 40 of the GDPR. The

draft establishes the types of research institutions and research that would qualify for data access under the Code. It lays out careful guidance regarding the steps both researchers and platforms must take to ensure they are in compliance with the GDPR. The draft also lays out a framework for evaluating the relative risks involved in processing different types of data and then connects each level of risk to a number of organizational and technical safeguards to be implemented by platforms, researchers, and research institutions.

Yet the draft contained in this report is just that—a draft. A few crucial issues remain outstanding before such a Code can become operational. First, Article 41 requires both a Code Owner and a Monitoring Body. The latter is required to monitor compliance with a Code and must be accredited by a relevant European Data Protection Authority. Neither of these bodies yet exists, and setting them up will require significant additional resources. Moreover, ultimately, any Article 40 Code of Conduct must be adopted and enforced by one or more Data Protection Authorities.

Before moving forward, we also believe that additional stakeholder input is crucial. With twelve members, the Working Group's small size permitted efficient and effective work. Though members of the Working Group did not always agree, we were able—despite very different interests and incentives—to reach consensus on the vast majority of the questions before us. Indeed, the Working Group made more progress in one year than we initially believed possible. However, now that we have successfully drafted a proposal that addresses many of the most difficult issues at hand, it is important that we stress-test its principles and proposed solutions with additional relevant stakeholders.

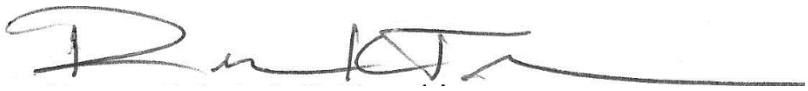
Finally, and perhaps most crucially, the draft Code represents what is currently possible under the status quo. Yet, one of the Working Group's clearest findings was that the status quo presents suboptimal conditions for platform-to-researcher data access. Most importantly, the Working Group reached consensus on the need and desire for an independent intermediary body that can perform a number of key governance tasks, such as reviewing and certifying platform codebooks, researcher proposals, and the safeguards put in place by each. The report explains the need for this intermediary body in greater detail.

In short, there is still much work to do. Nonetheless, I believe this report represents a major step forward in discussions of platform-to-researcher data access. The draft Code's guidance on GDPR compliance and its recommendations for how to evaluate, and, in turn, safeguard against, risks to data subjects offer new insights for researchers and their institutions, for platforms, and for policymakers and regulators alike.

Indeed, the EU is currently building a new framework that will legally oblige platforms to provide data to independent researchers, at a regulator's request, for the purpose of analyzing platforms' adherence to obligations in the Digital Services Act. The Working Group report is useful in this new regulatory context, offering a blueprint for how the modalities of data sharing can be organized in practice. Yet, the report will also be useful for those outside of Europe. Though certain requirements are tied to specifications under the GDPR, the general principles and proposed solutions the report provides are instructive in any legal context.

In closing this cover letter, let me take a moment to express my sincerest gratitude to the members of the Working Group, as well as to the team at AWO, who provided secretarial support and legal guidance for all of our endeavors. It has been a pleasure undertaking this challenge with each of you.

Sincerely,



Rebekah Tromble
Chair, EDMO Working Group on Platform-to-Researcher Data Access

I. Background and Motivations

Various third parties have consistently asked for improved access to data from platforms in order to assess the impact of platforms, including the impact of their design and policy decisions, and the impact of content that they host and disseminate, on individuals, social groups, institutions, and society. Calls for more data access have been ubiquitous across different fields and professions. More than 300 psychology scholars, for example, have argued that without such data it will be "impossible to identify and promote mental health in the 21st century".[1] Similarly, researchers in the field of online disinformation have stated that "data access would enable researchers to perform studies on a broader scale, allow for improved characterization of misinformation in real-world contexts, and facilitate the testing of interventions to prevent the spread of misinformation".[2]

Scientific research is intended to help us understand the world around us. It aims to identify trends, to monitor change over time, to build understanding of what is happening and why, and to develop and trial innovations that can improve society. As the communication, media, and information ecosystems have changed and evolved, so too has the nature of scientific inquiry. And yet, researchers' ability to study a growing and increasingly important element of the human experience is curtailed because of the limited availability of platform data. In particular, individual-level data are needed to build a better understanding of why observed phenomena are happening, who is affected, and what the effects entail.

At its core, scientific research requires individual-level data to understand and explain social phenomena. As an example, individual-level data can help to explain the conditions under which someone is likely to suffer mental health difficulties as a result of their online experiences and which, if any, forms of online intervention are most likely to help. In order to conduct causal research, scientific research needs non-aggregated, individual-level data that are often unfortunately effectively impossible to anonymize. The challenge of anonymization grows even greater when we seek to answer research questions over time. For example, if we want to understand the algorithmic vs. user-driven sources of potential online echo chambers longitudinally, the longer we analyse individuals' activities on one or more platforms, the more personal information their activities will reveal. Stripping their

[1] Letter of more than 300 academic researchers, available at https://www.oii.ox.ac.uk/an-open-letter-to-mark-zuckerberg/

[2] Irene V. Pasquetto et al., *Tackling misinformation: What researchers could do with social media data*, Harvard Kennedy School Misinformation Review, 9 December 2020, https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-could-do-with-social-media-data/

names, dates of birth, and so on won't achieve anonymization in practice. Additionally, if researchers seek to develop and trial innovations - for example, developing better classifiers to identify and ultimately help address online harassment - they need individual-level data at such scales and in such forms (e.g., text and images) that render anonymization effectively impossible.

In sum, in order to allow researchers to conduct much-needed causal inquiry, as well as other vital research that supports innovations and insights in the public interest, scientific researchers will need to have access to personal data. Quite simply, the ability of multi-disciplinary researchers around the world to conduct pioneering and socially important research is tied to the availability of these data.

Requests for access to data for scientific research purposes do not constitute an explicit endorsement of certain business models which have at their core the collection and exploitation of personal data, and requests for data access should not be interpreted as an incentive for platforms to collect even more data. Platforms are constantly conducting research based on the data they collect, but they very rarely share the results of these studies with the public and policymakers. Hence, requests for data access by scientific researchers acknowledge the information asymmetry between platforms and researchers, which currently prevents the development of knowledge that would be beneficial to our societies and lead to more evidence-based policymaking.

Since the adoption of the European Union's General Data Protection Regulation (GDPR), there has been extensive debate regarding its implications for the sharing of various forms of platform data for independent research purposes. Recognizing its broad societal value, the GDPR provides a special, more permissive regime for the processing of personal data for scientific research. The European Data Protection Supervisor has acknowledged the value of scientific research for democratic societies and affirmed the right of researchers 'operating within ethical governance frameworks' to process personal data.[3]

In the EU several platforms have themselves agreed to provide greater access to their data for independent research as part of the initial EU Code of Practice on Disinformation. However, researchers have voiced strong dissatisfaction with the steps taken under that Code of Practice, and formal evaluations of the implementation of that Code of Practice have found the platforms could do more to

[3] 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

ensure researchers' access.[4] Yet, in this and similar matters, platform representatives have repeatedly cited the GDPR as a barrier to sharing further data with researchers, arguing that the law is unclear about the mechanisms for, and legal implications of, data sharing. Indeed, many researchers themselves have echoed such concerns, noting that practices within their own research communities do not always foreground data ethics and data subjects' rights.[5]

II. A Path Forward

As intractable as this issue has often seemed, Article 40 of the GDPR provides a potential remedy and path forward.[6] Under Article 40, stakeholders may develop a Code of Conduct that lays out how the GDPR might be put into practice in a "specific, practical and precise manner". Such a Code, which must be approved by a relevant Data Protection Authority, could be specifically designed to address digital platform data access for independent research, as it may reduce the legal uncertainties and risks inherent for the platforms, while simultaneously offering researchers a clearer route to data access and laying out clear guidance for all parties on how to respect the rights of data subjects, as intended by the GDPR.

This report includes a draft proposal for such a Code of Conduct.

However, this is not an operational Code. Article 41 of the GDPR explicitly requires the set-up of a body that can monitor the compliance with a Code of Conduct pursuant to Article 40. Article 41.1 states that such a body needs to have "an appropriate level of expertise in relation to the subject-matter of the Code and [be] accredited for that purpose by the competent supervisory authority". No such monitoring body has yet been established.

[4] A new Code of Practice on Disinformation, which will include new commitments of signatories to provide access to data, is expected to be released in June 2022.

[5] See, for example, "Holding to Account: Safiya Umoja Nobel and Meredith Whittaker on Duties of Care and Resistance to Big Tech," *Logic Magazine*, December 25, 2021, https://logicmag.io/beacons/holding-to-account-safiya-umoja-noble-and-meredith-whittaker/. Members of the Working Group have also written on these issues, including, Rebekah Tromble, "Where Have All the Data Gone: A Critical Reflection on Academic Digital Research in the Post-API Age," *Social Media + Society*, January-March 2021, https://journals.sagepub.com/doi/full/10.1177/2056305121988929.

[6] Mathias Vermeulen, The Keys to the Kingdom. Knight First Amendment Institute at Columbia University, 27 July 2021, https://knightcolumbia.org/content/the-keys-to-the-kingdom

Moreover, to become operational, a Code must have a "Code Owner". Traditionally, Codes of Conduct are established by companies or organizations within a single sector or industry, and organizations representing that sector or industry as a whole are named "Code Owner". In this instance, however, the Code Owner must represent the interests of multiple stakeholders, including the platforms and researchers from both academia and civil society. Currently, no such organization currently bridges these categories of stakeholders, and thus, there is no natural Code Owner.

Lacking a natural Code Owner, the European Digital Media Observatory (EDMO) initially stepped in to initiate development of a Code of Conduct.

III. Processes and Procedures

EDMO brings together fact-checkers, media literacy experts, and academic researchers to understand and analyse disinformation, in collaboration with media organizations, online platforms and media practitioners. One of EDMO's objectives is to help members of its community access data for research purposes, including data digital platform data.

EDMO believed that there may be significant value in initiating a process to develop a Code of Conduct for the sharing of data between digital platforms and academic researchers in the EU. The process of working through the elements needed to construct such a Code was thought to have value in-and-of itself, if it brought all parties together to work through the legal questions and proposed solutions that they each believe are important.

Recital 99 of the GDPR states that in drawing up such a Code of Conduct, "associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations". As the only body in the EU that brings together many potentially relevant controllers, EDMO decided to launch an open call for comments on the 24th of November 2020 in which it asked for feedback about (a) whether the creation of such a Code could be helpful and (b) whether EDMO would be a suitable body to lead this process. EDMO envisioned the creation of a Working Group on Access to Data Held by Digital Platforms for the Purposes of Social Scientific Research ("Working Group") comprising 10-15 members from academia, industry, civil society, and relevant legal fields, with its chair selected by EDMO's Advisory Board.

The call for comments further included requests for feedback on the following topics:

- Analyses of legal or technical questions related to access to research data that the group would need to address;
- Expressions of interest from associations or individuals in contributing to the work of the group;
- Offers of resources to support the work of the group, whether in terms of direct financial contributions or help in-kind.

EDMO received a number of responses to this call from researchers, platforms, and civil society representatives that answered both questions (a) and (b) positively. EDMO therefore chose to proceed to establish the Working Group, whose composition and agenda were guided in large part by the feedback and suggestions received in the call for comments.

As a member of the EDMO Advisory Board and the Director of the Institute for Data, Democracy & Politics at George Washington University, and as a scholar with noted expertise on digital data ethics and platform data-sharing issues, EDMO appointed Dr. Rebekah Tromble as Chair of the Working Group. George Washington University subsequently secured philanthropic foundation funding to provide financial support for the Working Group.

The data rights agency AWO, led by Mathias Vermeulen and Ravi Naik, was retained to draft the Code on the basis of the guidance of the Working Group and to provide legal advice on the application of the GDPR to the Working Group.

The members of the Working Group are:

- Marta Cantero Gamito, University of Tartu
- Kate Dommett, University of Sheffield
- Charles Ess, University of Oslo
- Andrew Gruen, Meta
- Estelle Masse, Access Now
- Solomon Messing, Twitter
- Rebekah Tromble (chair), George Washington University, EDMO
- Cristian Vaccari, Loughborough University
- Claes de Vreese, University of Amsterdam, EDMO
- Katrin Weller, GESIS
- Clement Wolf, Google
- Gabriela Zanfir-Fortuna, Future of Privacy Forum

Based on feedback and suggestions received in EDMO's call for comments, AWO drafted a document in May 2021 describing the envisaged pathway towards the creation of an Article 40 Code of Conduct, and the potential topics such a code could

address. This document was discussed at the inaugural meeting of the Working Group on the 10th of June 2021, at which time the Working Group also discussed and adopted a set of bylaws governing its work and decision-making.
The Working Group met ten times between June and November 2021 to have focused discussions based on a number of briefing notes that were drafted by AWO on the following topics:

- What is “research”? Legal and practical considerations (27p). This briefing note outlined how the concept of “research” can be approached, drawing on legal and practical considerations.
- Navigating lawfulness – the legal bases for processing data (46p). This briefing note provides insights into the potentially applicable bases for data processing activities and explores how a Code can assist platforms and researchers with identifying and applying these legal bases.
- Roles and responsibilities – legal status for processing and its consequences (33p). This briefing note sets out the roles established by the GDPR and identifies the relevant legal and factual criteria that are likely to determine those roles in the specific context of platform-to-researcher data sharing.
- Security, safeguards and data protection by design and default: An overview of the legal requirements (19p).
- Jurisdiction and International Data Transfers: Navigating the extra-territorial reach of the GDPR (21 pages)

Both the academic representatives and the representatives of the platforms issued separate input papers on relevant topics during this timeframe, as well. Where appropriate, platforms have made various representatives available from their legal and internal research teams to talk to the Working Group.

Based on this extensive consultation, between January and March 2022, a draft Code was prepared by AWO and the Working Group chair, with input from members of the Working Group. Members of the Working Group submitted comments on several draft versions and discussed the final language of the draft Code as a group. A majority of the members of the Working Group subsequently approved the publication of this report, and all have expressed support for the next steps and future considerations described in Section IV. Several members of the Working Group have also appended concurrence letters to this report.

IV. Additional Findings

Though the majority of Working Group's most important conclusions and findings are reflected in the draft Code of Conduct itself, there are several issues we took up that require separate articulation and explanation.

A. Technical Standards

Where possible, the Code should point to specific standards and protocols for the implementation of technical safeguards. The Working Group considered, for example, whether to recommend (or require) that platforms and research institutions comply with specific cybersecurity standards, such as those laid out by the International Organization for Standardization. However, after interviewing a number of IT professionals at various European universities, as well as research organizations in Europe and the US, it became clear that no specific set of standards prevails for research institutions and that in many, if not most, instances, acquiring certification for these standards would be cost prohibitive and impracticable. Thus, additional consideration is required to help identify and lay out a set of minimum protocols and standards appropriate to universities and other research organizations.

B. Safeguards Considered but Not Recommended

Members of the Working Group considered some mechanisms for safeguarding data that, though not prohibited under the draft Code, the Working Group chose not to recommend.

1. Non-Consumptive Approaches

The HathiTrust Research Center (HTRC) allows researchers to perform analyses on a large trove of "texts in the public domain and under copyright in a manner that [is] secure and compliant with appropriate U.S. copyright law." To do so, researchers submit computational code to be run on data in a secure system. The output data can be exported, but the data being analyzed cannot. The HTRC does not permit the researchers to work within the secure environment to conduct and review the analyses. Nor can researchers view the underlying data.

This approach is appropriate for the HTRC use case, which must adhere to relevant copyright law, but is not practicable for access to platform data envisioned under this Code. Essential tasks such as data exploration and code debugging would be rendered impracticable, and, members of the Working Group concluded, this non-

consumptive approach would seriously jeopardize both the independence and integrity of the scientific research envisioned under the Code.

2. Differential Privacy

Differential privacy is a technique in which random noise is added to a dataset such that, mathematically, it becomes difficult to re-identify individuals within aggregated data[7]. Differential privacy has seen numerous applications, including for privacy-protection of social media data. Notably, Facebook applied differential privacy to an aggregated URLs dataset as part of the Social Science One initiative.[8]

However, differential privacy comes with significant limitations that may hamper research outcomes and study replicability, particularly for social scientific research that seeks to establish the representativeness of the data and generalizability of the findings. Researchers analyzing differentially private datasets work with a "privacy budget" that limits the number of analyses they can run. This limitation reduces the risk of re-identification. However, it also hampers exploratory research, which is particularly important in contexts where data cannot be widely shared. Differential privacy also makes it impossible, by definition, to replicate previous studies, as the random noise added to a dataset changes every time a new analysis is conducted, in turn altering results. Though in theory the results of any replication should be quite similar to those of the original study, in practice, the difference in outcomes may be significant enough to cast doubt on the initial results—doubt that may not be allayed with additional analyses that fall within either the original or replication study's privacy budget. Such challenges are particularly acute for research that seeks to analyze a relatively small dataset (or a relatively small subset of a larger dataset), since more noise must be added to smaller datasets.[9]

C. Code Flexibility

Though specificity is generally desirable in a Code of Conduct, and the draft Code provided here offers a much greater degree of specificity than offered in any other documentation and guidance for platform-to-researcher data access, the draft Code

[7] Dwork C., McSherry F., Nissim K., Smith A. (2006) Calibrating noise to sensitivity in private data analysis. In: Halevi S., Rabin T. (eds) Theory of cryptography. TCC 2006. Lecture Notes in Computer Science, vol 3876. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11681878_14.

[8] King, G. & Persily, N. (2020). "Unprecedented Facebook URLs dataset now available for academic research through Social Science One." https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one.

[9] Gondara, L., & Wang, K. (2020, August). Differentially private small dataset release using random projections. In *Conference on Uncertainty in Artificial Intelligence* (pp. 639-648). PMLR.

is crafted with overall flexibility in mind. Independent researchers do not know precisely what kinds of data the platforms currently collect that could become available for research purposes. Nor, of course, do they know how the platforms' practices for generating and collecting data will develop in the future, what services will be created, and what kinds of user actions and reactions they will generate. For this Code to be helpful for future research, guidance must be open, flexible, and forward-looking, rather than static and tied to the current state of the field.

D. The Need for an Independent Intermediary Body

As noted, for a Code to become operational, both a Code Owner and Code Monitoring Body must be identified (or established). One or more Data Protection Authorities must also adopt the Code. However, the Working Group identified another critical gap in the status quo: namely, the absence of an independent intermediary body that could help oversee and even implement the processes envisioned by the Code. Though not required under the GDPR, the Working Group concluded that such a body is critical to smooth functioning of platform-to-researcher data access.

As Parts I and II of the draft Code make clear, under the status quo, various requirements of and recommendations for both platforms and researchers will be considerably easier to undertake with an independent intermediary body in place. For example, as described in Parts I and II, both platforms and researchers must be satisfied that the proposed research meets a set of methodological and ethical criteria before any processing takes place pursuant to the Code. Though the Code lays out mechanisms to maximize the independence of the researchers and their work, under the status quo, independent review and verification of researchers and research proposals is not guaranteed. If, however, an intermediary body were established to facilitate independent review of researchers and research proposals - (a) certifying that researchers are qualified and competent to perform the research, (b) verifying that the research itself is qualified under the Code, and (c) providing these certifications to the platforms and any other appropriate parties - concerns about researcher and research independence could be substantially mitigated. Such a body might also review and certify, per Part II of the Code, that appropriate technical and organisational safeguards are put in place by both platforms and researchers. An independent intermediary body could also serve an advisory function to help facilitate access to data for researchers as provided for in Article 31.5 in the Digital Services Act.

Streamlining these review and certification processes and housing them within an independent intermediary body also has the benefit of reducing the burdens placed

on smaller, under-resourced universities and research institutions, subsequently opening data access to a much more diverse pool of researchers.

Here we provide a full set of functions the Working Group considers well-suited to an independent intermediary body:

- Reviewing codebooks developed by platforms, including reviewing the description of the data and the risk score the platform has assigned to the data (see Part II of the draft Code);
- Helping to inform researchers about the availability of specific data;
- Vetting researchers to ensure they meet the criteria laid out in the Code (e.g., are associated with an appropriate institution, in an appropriate role);
- Reviewing researchers' Research Proposals, including their Data Needs and Management Plan (see Part II of the Draft Code);
- Performing or facilitating required ethical and methodological reviews (see Part II of the draft Code);
- Maintaining a portal that provides public information about the research conducted under the Code and facilitates the exercise of data subject rights (see Part I of the draft Code);
- Facilitating and streamlining the identification of new data needs;
- Facilitating processes for translating those needs into new datasets and/or data access mechanisms;
- Facilitating changes or updates to existing datasets and/or data access mechanisms, including to enhance data usefulness and usability;
- Serving as Code Owner.

Though the EDMO Working Group did not have a mandate to consider or set up an independent intermediary body, members of the Working Group **strongly recommend the creation of such an organization**.

V. Draft Code of Conduct Overview

The Code is structured as follows: Part I of the Code sets out the requirements of the GDPR provisions as they pertain to research and clarifies how platforms and researchers should implement those requirements. Section 1 of Part I elaborates on the exemptions and Member-State derogations for research within the GDPR. Section 2 spells out the legal roles, responsibilities, and liability for both platforms and researchers. Section 3 provides clarity on the application of the most relevant legal bases for researchers' and platforms' processing under the GDPR. Section 4 highlights what types of safeguards the GDPR requires from a security perspective, while Section 5 highlights researchers' and platforms' transparency obligations and

data subjects' rights. Finally, Section 6 of Part I focuses on the jurisdictional scope of the GDPR and international data transfers.

Part II of the Code contains specific guidance on how platforms and researchers can meet their obligations to put in place safeguards for the protection of personal data, bearing in mind best practice in the scientific and historical research context. It highlights how this Code can be implemented in practice, using a scenario in which platforms make available codebooks (Section 2), which indicate to researchers what data may be available for qualifying research. After this release, a researcher formulates a research proposal (Section 3), including an assessment of the risk level of the research (Section 5), selection of safeguards (Section 6), and methodological and ethical review (Section 7). In our proposed Part II, the platform reviews the proposal (Section 8) to ensure that it is for qualifying research and that the proposed safeguards are appropriate. (However, the Working Group strongly recommends that, in the future, this function be assigned to an independent intermediary body (see IV.D above).) After this process, the parties may enter into a data sharing agreement that incorporates the details of the research proposal and binds them to implementing the agreed safeguards. Annex 1 provides a checklist for researchers to confirm when they are ready to submit a request for data sharing to a platform, whereas Annex 2 provides a checklist for platforms to confirm they have sufficient information to enter into a data sharing agreement and share data. A template for assessing legitimate interests in research processing is included at Annex 3. Finally, Annex 4 contains a compendium of relevant Member State laws in 10 research-intensive jurisdictions where the GDPR applies.

VI. Concurrence Letters

- Gabriela Zanfir-Fortuna, Future of Privacy Forum
- Twitter
- Meta

May 30, 2022

I commend my colleagues from the EDMO Working Group, our Chair - Rebekah Tromble, and Secretariat - AWO, for taking upon themselves to solve one of the biggest questions in data protection of our time: Is conducting research compatible with the GDPR? If so, what kind of research? And how are they compatible?

Under the guidance of Recital 4 of the GDPR, which is probably the key to all legal interpretation of this Regulation, I am of the opinion that processing personal data for research purposes is not only compatible with the GDPR, but that it is actually encouraged and facilitated by it. Recital 4 tells us that "the processing of personal data should be designed to serve mankind". If the GDPR would be a barrier to research which is based on processing of personal data, its fundamental goal of supporting the processing of personal data in a way that it serves mankind would be undermined. To be sure, as the Preamble of the draft Code clarifies, qualifying research under its scope must have as its explicit aim "the development of society's collective knowledge".

There is no clearer evidence that the GDPR facilitates processing of personal data for research purposes than the "compatibility presumption" it encodes in Article 5(1)(b), which establishes that processing of personal data for the purposes of scientific research is a compatible purpose with whatever initial purpose the processing had. In practical terms, this means that one of the most burdensome GDPR compliance obligations for controllers – that of ensuring the processing has a lawful ground in place, is alleviated for processing of personal data initially collected and used for other reasons when it is further relied on for scientific research purposes. At a high level, the existence of this overarching presumption of compatibility also means that the GDPR envisaged all personal data available for processing could potentially be relied on to conduct scientific research.

However, this presumption of compatibility is by no means a blank check. In fact, as the European Data Protection Supervisor explained in its Preliminary Opinion on Data Protection and Scientific Research[1], this presumption directly depends on the

[1] Available at https://edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf, last accessed May 30, 2022.

requirement to ensure appropriate technical and organizational safeguards, such as pseudonymization and access limitations, pursuant to Article 89(1) GDPR. Moreover, any such secondary, compatible processing must respect all of the other rules in the GDPR – from data minimization to retention limitation, to ensuring appropriate data security, transparency and making possible the exercise of the rights of the data subject and so on.

Those responsible to comply with the panoply of data protection safeguards and liable under data protection law when conducting scientific research are the controllers. But who are the controllers in this situation? It is crucial that researchers and their organizations also understand that they must only process personal data within the framework designed by the GDPR and Article 8 of the EU Charter of Fundamental Rights (the fundamental right to the protection of personal data). In the particular situation of platforms sharing personal data for research purposes with researchers, both the platforms as Data Sharing Organizations and the researchers as organizations processing personal data obtained from platforms have distinct legal obligations and they are both responsible for respecting the fundamental right to the protection of personal data within their remit.

While the draft Code may not solve all of the issues stemming from this dual relationship platforms – researchers, which involves making personal data available and then using it for scientific research, it is the most complex and nuanced exploration of the issue I am aware of and I am proud to have been part of the EDMO Working Group and contribute to this debate. I believe that regardless of whether it will become in the end a Code of Conduct or not, this draft advances reaching practical solutions ultimately to be accepted by platforms and researchers alike not only under the GDPR as it aims to do, but perhaps also under the future Data Services Act, and it moves the debate forward.

Sincerely,

Dr. Gabriela Zanfir-Fortuna
Member of the EDMO Working Group

GZanfir

30 May, 2022

Twitter, International Unlimited Company
1 Cumberland Place
Fenian Street, Dublin 2,
Ireland
D02 AX07

Registered Number:
503351

Directors:
L. O'Brien,
S. McSweeney
S. Edgett (US)

Object: Concurring Opinions Letter on the Report of the EDMO Working Group on Platform-to-Researcher Data Access

Transparency is at the heart of what we do at Twitter and we have always sought to facilitate researchers' access to our platform's data. Since 2006 Twitter has had an open API allowing developers and researchers to use data from the public conversation to study diverse topics, such as state-backed efforts to disrupt the public conversation, floods and climate change, attitudes and perceptions about COVID-19 and efforts to promote a healthy conversation online. While the tool has been developed and improved over the years, our commitment to transparency and researchers' access to data remains steadfast.

We appreciate the opportunity to engage in EDMO's important work on this issue. Our concurring opinion on the work that has been done to date and a clarification of our position can be found below.

The **original aim of the Working Group** was to put together a guidance report for the future creation of a Code that would contain the main parameters and conditions to allow researchers access to digital platform data. In this context, important considerations about the ethical and privacy implications of sharing such data were discussed.

We believe this effort has advanced the conversation about how to legally and effectively go about sharing data under the General Data Protection Regulation (GDPR). In particular, it provides a number of useful clarifications and risk-mitigation strategies. However, the establishment of an independent intermediary body, as discussed in the draft Code, will be critical to ensure effective operation and governance. Such an entity will be necessary to continue to make progress to resolve legal questions, establish additional protocols to ensure responsible use of data, review research and study protocol eligibility.

Throughout the process, **Twitter has been committed** to the task of the Working Group, to **explore the key issues** around the possibility of facilitating data access to researchers in a way that is compliant with the GDPR. We support the principle of transparency and the importance of giving researchers access to platform data.

The report agreed by the Working Group contains a draft Code that represents a **step forward** in discussions of platform-to-researcher data access. However, **more work is required,** as the principles will have to be

further examined by a wider pool of experts and **additional legal review is needed before it could be adopted as a Code.** This underscores the need for an independent intermediary body, which we hope can make progress in addressing specific issues below.

Some areas in which further work is needed include inter alia:

- Additional privacy and data protection protocols are necessary. Twitter has always been careful to impose limits on how the data that is shared through our APIs is used. Researchers and developers must agree to our developers agreement and prohibited use cases. Any Code or guidelines should also address similar issues.
- While the draft Code provides a great deal of clarity related to how research can take place under GDPR, there is still considerable uncertainty surrounding the legal implications and responsibilities of both DSOs and researchers when processing what the GDPR defines as Special Category Data (SCD). A great deal of social science and humanities research entails processing what is defined as special category data and thus we would expect much of the research that will take place will trigger SCD related complications (Article 9 and 89).
- The draft Code provides additional clarity surrounding what activities comprise “research” and what kind of entity can carry it out; however more work is necessary. The Code currently specifies that research must be conducted by an “entity which has as one of its principal aims the conduct of research on a not-for-profit basis […]” This leaves open opportunities for entities whose principal aim is not the conduct of research to advance knowledge via peer-reviewed publication as is generally the case for university researchers, but for organisations whose goals include advocacy oriented research for the purpose of shaping public dialogue or influencing public opinion.
- The guidance surrounding the research exemption to storage limitation creates ambiguity for platforms and needs further work. Platforms/DSOs have built data retention systems that comply with existent regulations, often at great expense. However, the guidance here is to “take a pragmatic approach to retaining data that is likely to be processed for research purposes, for example, where a major event, election, conflicts, political crises, war, or other exceptional circumstances […]”. Yet researchers generally need data across long periods of time, comprising both epochs of calm and conflict to make sense of these events. They often wish to analyse data from experiments conducted on the platform, or merge long-running platform data and survey data. Thus, it seems difficult to reconcile the guidance to save data that may be relevant to research, which is broader than what the Code assumes here, with the existing regulatory frameworks surrounding data retention.

Meta

30 May 2022

Professor Rebekah Tromble
Chair, EDMO Working Group on Access to Platform Data

Dear Professor Tromble,

Meta congratulates the EDMO Working Group on publication of this Report, which shows both progress toward the group's objectives as well as the need to continue working on essential issues to create a Code of Conduct that participants can implement and data protection authorities can approve. Meta continues to support the development of a Code of Conduct that will facilitate voluntary data sharing for scientific research while protecting the fundamental rights of individuals in Europe. We appreciate the opportunity to have contributed to the Working Group's efforts to date.

The Report demonstrates the progress the Working Group has made toward unpacking questions around the application of the GDPR to scientific research and data sharing by organizations. It addresses the important role that all parties, including researchers, research institutions and data sharing organizations, play in safeguarding data shared for scientific research. It also advances the discussion by proposing a methodology for determining how safeguards should be calibrated to different levels of risk in research contexts. We hope these discussions are carried forward into those on the forthcoming Digital Services Act.

Importantly, the Report recognizes the need to create an independent intermediary body to review research proposals submitted by researchers and codebooks created by data sharing organizations. Meta supports creating such a body as part of the text of the Code of Conduct.

Without such a body, organizations will continue to face uncertainties regarding the legality of data sharing for research and the scope of liability each party is exposed to in the context of data sharing. Particularly, organizations face real concerns about the data they share being misused or not adequately governed, including by being transferred onward or propagated in less secure environments. Without an independent review body, organizations will need to ensure that researchers adequately address these risks. Yet such a review by organizations is in tension with researchers' interest in preserving their own independence. An intermediary body can help to ensure appropriate governance over data shared for research – which addresses these core concerns about data security and privacy – without giving data sharing organizations control over the substance of research.

We are eager for the Working Group to continue its efforts to develop a Code of Conduct to achieve the following aims:

1) **Allocate responsibilities between researchers and data sharing organizations to ensure that each party is responsible for compliance with its GDPR obligations.**

2) **Create an independent intermediary body to vet each stakeholder's compliance with its respective obligations leading and pursuant to the data sharing. Importantly, data sharing organizations should not be tasked with assessing the scientific, methodological or ethical merits of research proposals, while researchers and research institutions need not face the burden of vetting organizations' data pipelines or codebooks.**

3) **Clearly define the qualification of researchers who may apply for access to data under the Code.**

4) **Obtain regulatory approval from data protection authorities, according to the process set forth in Articles 40-41 of the GDPR, to ensure that data sharing under the Code of Conduct conforms with the requirements of the GDPR, including those on legal bases to share data, data transfers and individual rights.**

The Working Group is well placed to achieve these aims, and we look forward to continuing to work with the group toward the development of an approved Code of Conduct that will facilitate secure and privacy protective scientific data based research.

We look forward to continuing our work.

EDMO (Draft) Code of Conduct for Platform-to-Researcher Data Sharing

Table of Contents

Preamble

Purpose of the Code

1. Researchers require access to data – including personal data, governed by the EU General Data Protection Regulation (GDPR)[1] – held by digital platforms for research into (inter alia) the use, role and impact of these platforms in society. This includes research into the impact of platforms' design and policy decisions, and the impact of content that they host and disseminate, on individuals, social groups, institutions and society. Such research benefits society as a whole and is to be encouraged and supported.

2. Platforms' caution about their GDPR obligations can be a barrier to their making data available to researchers, who also need to be mindful of their own obligations in respect of data processing[2]. However, respect for personal data is wholly compatible with responsible research. Indeed, the GDPR provides a special regime for data processing for research purposes.

3. Platforms acting as data sharing organisations ('**DSO**s') and researchers need confidence in their ability to share data in a way that is compliant with the GDPR. DSOs and researchers must understand their legal obligations. Both must also understand the safeguards that they will need to put in place to protect the data that DSOs share for research purposes.

4. The purpose of this proposal for a Code of Conduct for Platform-to-Researcher Data Sharing ("Code") is to clarify how the GDPR applies in the research context, to facilitate research, and to promote greater trust between DSOs and researchers regarding the sharing of data.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[2] Recital 159 GDPR provides: "For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."

5. **The Code is intended to be a Code of Conduct under Article 40 GDPR.** DSOs and researchers can become signatories to the Code to demonstrate their adherence to its requirements and to the GDPR.

6. Once approved, the Code, together with an accompanying data sharing agreement, could also serve as a **transfer mechanism under Article 46 GDPR.**

Application and Scope of the Code

7. The GDPR provides for a regime for the processing of personal data for the purposes of 'research'. The GDPR does not define 'research' but it encourages a broad approach to the concept. This Preamble clarifies what activities and purposes can be considered research (herein "**qualifying research**") under the Code and therefore benefit from the research regime.

8. Qualifying research is limited to a subset of data processing for research purposes to increase certainty and aid in the practical application of the GDPR.[3] However, the absence of an activity or institution from the scope of this Code must not be construed as a blanket statement about whether such activity or institution may fall within the scope of the research regime in the GDPR. A civil society organisation may, for example, request DSO data for an ad hoc research project. If the organisation and project did not meet the Code's definition of 'qualifying research', it would fall outside the scope of the Code. Nevertheless, such data sharing may still be considered processing for the purposes of research within the meaning of Recital 159 GDPR. Where these situations arise, the Code may be useful guidance, but DSOs and researchers will need to rely directly on provisions of the GDPR.

[3] To the extent that parties' personal data sharing for research purposes falls outside the scope of the Code, they will still need to ensure it complies with the GDPR.

9. The Code is not designed for research projects that process health data[4] or traffic and communications data[5] due to significant variation in EU Member States' legal frameworks on such data. The Code may apply to the processing of health data, but parties must independently satisfy themselves as to the relevant Member State law governing those projects.

10. Processing for research purposes will often involve the generation of inferences about individuals. For the avoidance of doubt, an inference about an identifiable individual, regardless of its accuracy, constitutes personal data for the purposes of the Code.

Qualifying Research

11. Whenever the Code is invoked, the parties involved will need to satisfy themselves that the proposed activity is 'qualifying research' under the Code. This will be a case-by-case determination that considers:

12. The **purpose** of the research:

    a) An explicit aim of the research must be the development of society's collective knowledge. While commercial entities may benefit from the research, the furtherance of commercial interests cannot be a main objective of the project.

13. The **entity(ies)** that will carry out the research[6]:

[4] Article 4.15 GDPR defines this as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". See also recital 35 of the GDPR.

[5] As defined in Directive 2002/58/EC (the ePrivacy Directive)

[6] Where data is to be shared with a consortium of organisations, each of them must fulfil these criteria.

a) The research must be carried out by an entity which has as one of its principal aims the conduct of research on a not-for-profit basis[7] pursuant to a state-recognised public-interest mission

b) access to the results generated by the research must not be enjoyed on a preferential basis by any entity that exercises a decisive influence (for example through control of funding, staffing or governance) upon the organisation.

c) The research entity must be able to explain its decision-making processes and funding structure, which includes the source of the entity's funding, and the source of funding for the specific research project that relies on the Code.

d) The entity must not carry out any of the following functions:

   i) Law enforcement;

   ii) Intelligence services; or

   iii) Defence, promotion or upholding of national security.

e) The entity must be meaningfully independent in the conduct of its affairs from any public body carrying out the functions listed in para 13(c) above.

14. The field of enquiry:

a) The Code applies broadly to research in the natural sciences, social sciences, humanities, computer science, engineering, and other fields as and when such research meets the other scope conditions described herein.

[7] The use of "non-for-profit" here includes entities that reinvest all profits in research or other public aims.

15. The research must comply with the following **methodological and ethical standards**:

    a) It must meet generally accepted ethical and methodological standards in scientific and historical research, including review of the ethical issues raised by a research proposal and peer review of the proposed methodological approaches, as described in Part II of the Code.

    b) The research should follow the Ethical Guidelines for Internet Research of the Association of Internet Researchers (as well as any other specialized or sector-based guidelines relevant to the research) and be reviewed and approved before data is requested from a DSO by an institutional, or appropriate third-party, ethical review board, as described in Part II of the Code.

    c) The research must be carried out on the basis of a Data Needs and Management Plan that has been reviewed and approved by an institutional, or appropriate third-party, Data Protection Officer, as described in Part II of the Code.

16. The Code applies to the sharing of data for specific research project(s), with specific research objectives set out at the time that data is requested under it[8]. The Code is not intended to apply to the further processing of that data for other research projects, or for other purposes, beyond the original research objectives. In situations where parties are engaged in such further processing, parties may rely on the GDPR to govern that processing, or may reapply the Code to that new research processing.

Structure of the Code

[8] Where access to data is required in order to define research questions, this should be defined as a research objective and the Code invoked in relation to this exploratory research project.

17. The Code brings together the GDPR's provisions concerning research into one place, demonstrating how data can be processed in compliance with that regime. It addresses how DSOs and researchers should approach the delimitation of their legal roles (controller, joint controller, processor), their responsibilities, liabilities, purposes, and legal bases for their processing. It also addresses the requirements regarding data transfers, data security and safeguarding requirements and data subject rights, which DSOs and researchers need to be aware of.

18. The Code is structured as follows:

    a) **Part 1** of the Code sets out the requirements of the GDPR provisions as they pertain to research and clarifies how DSOs and researchers should implement those requirements.

    b) **Part 2** of the Code contains guidance on how DSOs and researchers can implement the Code, focusing on a typical project scenario. It provides specific guidance on how to select and implement safeguards in the security of processing that are appropriate to the risks involved in the research.

Glossary of terms

19. Personal data (also referred to as "**data**" throughout the Code) is defined by Article 4(1) GDPR:

    "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

20. **Pseudonymisation** has the meaning given to it in Article 4(5) GDPR and 'pseudonymous' should be read accordingly:

    "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"

21. **Processing** has the meaning given to it in Article 4(2) GDPR:

    "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

22. A **data sharing organisation** or **DSO** is any data controller from whom data are requested pursuant to the Code for the purposes of qualifying research.

23. A **researcher** is any organisation or individual who requests access to data pursuant to the Code for the purposes of qualifying research. Part I of the Code deals with the obligations of data controllers and processors, and in Part I the term 'researcher' generally refers to an individual or entity acting as a data controller or processor under the GDPR, except where the context indicates that individual researchers are referred to.

24. When a requirement of the Code is mandatory and must be implemented by DSOs and researchers, the term "must" is used within the Code.

25. The Code also provides DSOs and researchers with guidance and best practice suggestions on how those mandatory requirements can be practically implemented, indicated by the words ‘should’, ‘may’, and ‘can’.

Part I

Section 1: The Research Exemptions

1A - DSOs and researchers must have regard to the unique position that research holds in EU data protection law, illustrated by the exemptions and derogations provided for research in Articles 5(1)(b), 5(1)(e), 9(2)(j), 14(5)(b), 17(3)(d), 21(6) and 89(2) GDPR.

1B - DSOs and researchers must ensure they can demonstrate that, where they rely on an exemption or derogation, such reliance on that research exemption or derogation applies both to the relevant processing activities and in the jurisdiction to which those activities are subject.

1C - DSOs and researchers must use this Code to govern data processing for the purposes of facilitating and carrying out qualifying research. The objectives of the qualifying research must be identified prior to any processing under this Code.

1D - DSOs and researchers must have regard to Member States' laws which aim to reconcile the right of data protection and freedom of expression and information under Article 85 GDPR.

1E - For DSOs, facilitating qualifying research is a compatible secondary purpose of processing under Article 5(1)(b) GDPR (subject to Member State law).

1F - This code may not be relied upon for data processing not carried out for the purposes of the qualifying research.

1G - DSOs and researchers must ensure effective and enforceable appropriate safeguards under Article 89 GDPR are in place for all data processing activities that rely on the research exemptions.

1H - DSOs should identify, among their employees, individuals or teams whose role includes the proactive facilitation of qualifying research by maintaining an open dialogue with researchers.

Explanatory Notes to Section 1

Introduction

1. DSOs and researchers should note that the GDPR exemptions and derogations for research[9] are not absolute or indefinite. They must only be used for explicit and specified research purposes and with due regards to jurisdictional considerations (as discussed in Section 6). Furthermore, "appropriate safeguards" must be in place before an exemption or derogation is relied on, pursuant to Article 89(1) GDPR. Such safeguards will include, for example, putting in place measures for transparency and the exercise of data subject rights (see Section 5) as well as safeguards in the security of processing (see further in Section 4 and Part II)

2. The GDPR "research exemptions" may be split into (i) **exemptions**, which do not require further implementing legislation; and (ii) **derogations** that require further implementing legislation in EU or domestic laws.

Exemptions

3. The exemptions to purpose limitation, storage limitation, transparency obligations, the right to erasure and the right to object do not require further implementation in EU or Member State law. These exemptions are found in the following articles of the GDPR:

    a) **Article 5(1)(b) GDPR** provides that personal data must only be processed for "*specified, explicit and legitimate purposes*". Personal data cannot be "further processed" for purposes that are incompatible with those primary purposes. There is a presumption however that research is a compatible secondary purpose (the "**presumption of compatibility**"). Member State law may attach conditions to the reliance

[9] Articles 5(1)(b), 5(1)(e), 9(2)(j), 14(5)(b), 17(3)(d), 21(6) and 89(2) of the GDPR contain the exemptions and derogation clauses for data processing for research purposes.

on this presumption – see the compendium of Member State laws at Annex 4.

b) **Article 5(1)(e) GDPR** contains an exemption for research that permits data to be stored for "*longer periods*" where it is being processed for the purposes of qualifying research. Whether "longer periods" are appropriate will depend on the characteristics of a given research project.

c) **Article 14(5)(b) GDPR** contains an exemption for research to transparency obligations where data are not obtained directly from the data subject. Articles 12, 13 and 14 of the GDPR contain the modalities of transparency. (See more on transparency in Section 5.)

d) **Article 17(3)(d)** states that the right to erasure will not apply if it "*is likely to render impossible or seriously impair the achievement of*" research objectives where the data processing is conducted in accordance with Article 89(1). The applicability of this exemption to researchers is considered further in Section 5.

e) **Article 21(6)** provides an exemption to the right to object where data processing for research "*is necessary for the performance of a task carried out for reasons of public interest*".

Derogations

4. The EU and its Member States may implement derogations under Article 89(2) to restrict individuals' right of access, right of rectification, and right to restriction for data processing for research. DSOs and researchers should therefore (i) identify the relevant laws to which their processing activities are subject (see Section 6), and (ii) refer to the compendium of Member States laws at Annex 4 for more information on implemented derogations.

Qualifying Research

5. Both DSOs and researchers will need to be satisfied that research is qualifying before any processing takes place pursuant to this Code. This may be through:

    a) Joint agreement between DSOs and researchers or research institutions – for example in a data sharing agreement – on the research objectives and methods for explicitly collaborative research;

    b) Disclosure by the researchers of their objectives and methods; or

    c) Assurance (e.g., by a third-party body) to DSOs that research is qualifying for the purposes of this Code.

Phasing projects

6. Researchers will not always know their research objectives in full in advance. For instance, they may need access to data as part of an exploratory phase in which they will further refine their longer-term research questions. In such cases, the parties may consider the distinct phases of the research project, applying the Code at each stage:

    a) Initially to facilitate access to data supporting exploratory qualifying research, where the researcher's objectives state the broad questions or issues to be explored and how the data will support identification of more detailed research questions and methodologies; and

    b) Once the main research questions have been identified, to facilitate access to data that enables researchers to answer them.

7. Whilst the invocation of the Code should occur at each stage, when relying on the Code in relation to the principal research questions the parties should be able to streamline its application by focusing on any material changes between the exploratory and the full research phase. For example, the focus of the second stage should focus on the material changes where the researcher requires

access to different data, if additional controllers will be involved, or if the full research objectives indicate a higher level of risk or sensitivity to the research.

8. DSOs should identify individuals or teams within their organisation and task them with facilitating qualifying research through this Code. Consistent points of contact and regular dialogue between DSOs and researchers (including representative bodies of researchers) will aid DSOs and researchers in more effectively carrying out research in compliance with their obligations under this Code.

Researchers

Purpose limitation

9. Researchers must only process the data shared under this Code the qualifying research they specified when making their request for data, which is their primary purpose. Researchers may not rely on the presumption of compatibility for any processing for a secondary purpose. The primary purpose will likely include:

    a) Facilitating replication of research findings by an independent peer reviewer;

    b) The outsourcing of routine data labelling work to processor third parties;

    c) Publication of research findings in journals and reports;

    d) Data archiving for scientific purposes;

    e) Complying with open-access requirements where these have been made known at the outset of a project.

Storage limitation

10. Researchers may rely on the storage limitation exemption. At the outset of their research project, researchers should set storage periods that are appropriate according to the research objective(s). Insofar as the duration or scope of their

project evolves, researchers should weigh the proportionality of extending the storage periods against the impact this may have on data subjects' rights. A record of the decisions taken about storage periods and the rationale for those decisions should be kept by all parties involved and updated as the research progresses.

11. However, researchers must be able to demonstrate the proportionality of extended storage periods, with reference to the needs of the project and the data involved, along with appropriate technical and organisational measures needed to safeguard data subjects' rights and freedoms.

12. For more information, see the Member States laws compendium at Annex 4.

Transparency obligations

13. Researchers who obtain data directly from data subjects must provide them with all the relevant information pursuant to Article 13 GDPR.

14. If researchers obtain personal data *indirectly* via DSOs, they will be able to rely on the Article 14(5)(b) exemption, where and insofar as one of the criteria listed at para 121, Section 5 is met.

15. If a researcher can demonstrate that one of the criteria applies, the exemption may only be relied on to the extent that it is proportionate to the impact on data subjects' rights. Proportionality should be assessed at the outset of a research project and reviewed periodically as the project evolves.

Articles 85: Member State-only derogations

16. Domestic legislatures may implement derogations for processing activities for "academic" purposes under Article 85(2). These will only apply in the respective jurisdictions where the derogations are implemented. Researchers should identify the jurisdiction applicable to their activities (see Section 6) and consult the Member States laws compendium at Annex 4 for further information.

DSOs

Purpose limitation

17. A DSO may rely on the presumption of compatibility to further process data for a "*specific, explicit and legitimate*" secondary purpose (subject to any qualifications in Member State law). Processing data to facilitate qualifying research under this Code meets this test. A DSO may therefore rely on the presumption of compatibility to further process data in support of qualifying research. It may do this by making data available directly to researchers for specific qualifying research projects, or by making data available to a third-party intermediary on the condition that data are used for qualifying research.

Storage limitation

18. The research exemption to storage limitation operates only "*insofar as the personal data will be processed solely*" for research purposes. A DSO may benefit from this exemption "*insofar*" as it facilitates specified and explicit research objectives. For example, in certain circumstances, data may need to be retained for "longer periods" for reproducibility/replicability purposes. Whilst data may not be retained on a purely speculative basis, DSOs should take a pragmatic approach to retaining data that is likely to be processed for research purposes, for example, where a major event, election, conflicts, political crises, war, or other exceptional circumstances[10] have taken place. DSOs should remain in dialogue with a broad range of representatives from the research community to aid its understanding about what types of data are likely to be in demand for research and therefore may be retained for longer periods. As more research takes place

[10] Extraordinary circumstances may entail "any unforeseeable event, such as earthquakes, hurricanes, pandemics and other serious cross-border threats to public health, war and acts of terrorism, where, for example, online DSOs may be misused for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information." See 2020/0361 (COD) Recital 71.

pursuant to this Code, DSOs' justification for retaining data likely to be of interest to researchers will be reinforced.

Transparency obligations

19. Where a DSO processes personal data that has not been collected directly from data subjects (e.g., where data are provided by researchers as part of a collaborative research project) and then processes the data for research purposes, then it may benefit from the research exemption under Article 14(5)(b). For more information on how to meet transparency obligations and the exemption, see Section 5.

Additional considerations regarding exemptions

20. Depending on the legal basis relied upon for processing, research exemptions, including those that do not require implementation in Member State law to take effect, may be modified by Member State law (see Annex 4).

21. EU Member States and EU institutions may provide further derogations for research, which may also limit data subjects' right to access, rectification, and restriction. However, those exemptions will only apply "*in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*". These standards are considered further in Section 5, and in Annex 4.

22. Domestic legislatures may implement derogations for processing activities for "academic" purposes under Article 85(2). These will only apply where the derogations are implemented in domestic laws. DSOs and researchers should consult the compendium at Annex 4.

Section 2: Legal Roles, Responsibilities and Liability

2A - The GDPR creates three legal roles for entities that process personal data: (i) data controllers, (ii) joint controllers, and (iii) data processors. The controller has primary responsibility for demonstrating compliance with the GDPR. The controller is the entity determining the purposes and means (the why and the how) of processing. Before processing data, DSOs and researchers must understand their legal status under the GDPR in relation to each processing activity for research within the scope of this Code.

2B - When considering their legal status, DSOs and researchers must apply the concepts of controller and joint controller broadly to ensure the effective and complete protection of data subjects' rights.

2C - DSOs and researchers must enter into data sharing agreements appropriate to the entities and their relationship to each other, which requires those parties to correctly identify and accept responsibility for the data processing they will carry out under their identified legal status.

Explanatory Notes to Section 2

23. Individuals or entities that process data have legal status under the GDPR. An actor's legal status is based on a factual analysis of its role in relation to processing, rather than any contractual term or self-appointed position.

24. Different obligations and responsibilities arise depending on an actor's legal status. As such, understanding their legal status under the GDPR must be a primary consideration for DSOs and researchers. They should consider their legal status in advance and document their intentions and understanding in their data sharing agreement.

<u>Controller and Joint Controller</u>

25. The "controller" is the primary entity responsible for compliance with the data protection regime. The "controller" is defined in Article 4(7) GDPR as

> *The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*

26. The type of entity that can be considered a controller includes natural and legal persons and any "other body". However, where an individual processes data as part of their role within a corporate structure, the corporate entity is considered the data controller in order to provide data subjects with a more stable and reliable reference point from which to exercise their rights.

27. Therefore, where an employment relationship exists between the institution and an individual researcher, the institution that they are affiliated with, not the individual researcher, will be the controller. Where the affiliation between the institution and researcher is more tenuous or complicated, individual researchers should consider whether they may personally be controllers under the GDPR (i.e., whether they, independently of their institution, are determining the purposes and essential means of processing).

28. Further, if individual researchers use personal data for their own purpose beyond the boundaries and control regime set by an institution, they will be controllers.

29. If controllers have the same purposes and decide the purposes and means of processing together, they will be in a "joint controller" relationship for that processing. A shared interest in the purpose of the research can be evidenced by a shared interest in the objective of the research project.

30. European Courts have taken an expansive approach to when joint controller relationships arise. For instance, an entity does not need access to the data being processed to be considered a joint controller. However, controllers will not be joint controllers if they are processing the same data for different purposes.

Processor

31. The GDPR also recognises that actors may process data on behalf of and on the instructions of a controller. Such entities are recognised as "processors", defined in Article 4(8) GDPR as

> *A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

32. Processors only act on behalf of a controller. They must enter into a written agreement with controllers that sets out (i) the "subject matter and duration" of the processing to be undertaken, (ii) the specific purpose of the processing, (iii) the security measures to be implemented, and (iv) other matters set out in Article 28(3) GDPR. Processors have fewer obligations than controllers.

33. Processors should guard against taking any steps to determine the purposes and means of processing, as this may result in them acting as controllers in those processing activities.

Determining legal status for DSOs and researchers

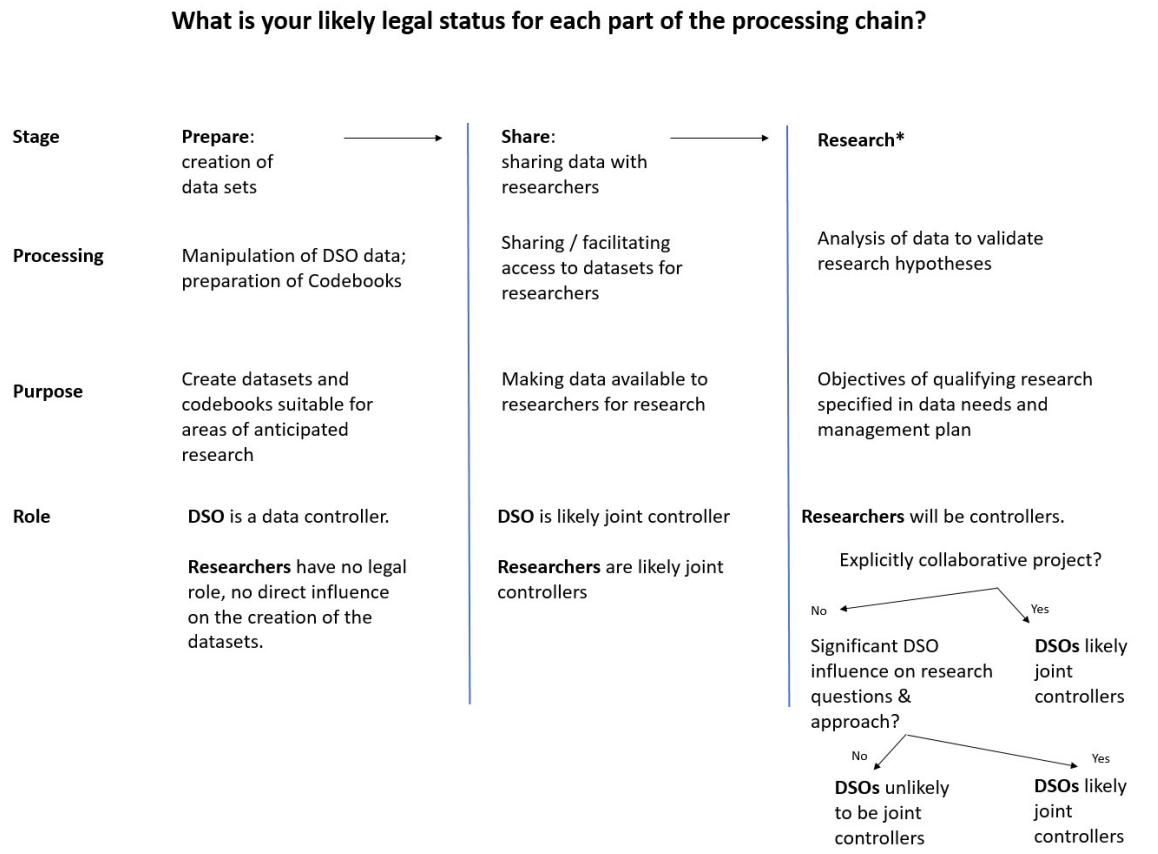
34. DSO-to-researcher data sharing is likely to involve several distinct processing operations, such as (i) processing by the DSO to make the data available to the researcher, and (ii) processing by the researcher to access and subsequently conduct research using that data. When planning research projects, DSOs and researchers must identify the distinct processing activities that will take place and identify the controllers, joint controllers and processors (if any) for each processing activity.

35. The parties' legal status will depend on (i) the nature of the processing and (ii) the relationship between the parties. The European Data Protection Board (EDPB) recognise that:

> *the concept of a controller can be linked either to a single processing operation or to a set of operations. In practice, this may mean that the*

control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.

36. This can be applied in the DSO to researcher context as follows:



DSOs

37. DSOs will be data controllers for their primary processing activities. When sharing data with researchers, DSOs may find themselves playing any of the three roles:

    a) **Controllers** – DSOs are likely to determine the "purpose and means" of how data are (i) prepared for sharing, and (ii) made accessible to researchers. In most cases, the purpose will be to facilitate a given research project and the means will be dictated by the DSO, whether by

direct transfer to the researcher or through a secure data sharing environment. Thus, DSOs will likely be data controllers for the processing activities involved in sharing data with researchers. Whether a DSO is a controller for subsequent processing will depend on the specific characteristics of the research.

b) **Joint controllers** – Where DSOs and researchers collaborate on research projects, both parties are likely to agree on the reasons and methods for the research. This may result in joint controllership. The key question is whether DSOs and researchers decide the purposes and means of processing together. Facts to consider include: (a) the degree of influence exercised by the DSO over the researchers' processing; and (b) the benefits, financial or otherwise, that the DSO derives from the processing. The DSO need not perform an equal amount of processing nor access the data to be considered a joint controller. However, a DSO will not be a joint controller merely because it mandates detailed data access and security requirements, as these are non-essential means of processing.

c) **Processor** – In certain circumstances, the DSO may act as a data processor for a researcher. For instance, a researcher might develop a project with disparate sources of data and then request a DSO to process a part of that dataset. If the DSO were to follow instructions from the researcher and only process the data for those limited purposes, then they may be considered a processor. This scenario, however, is not likely to occur often and would require detailed scrutiny of the facts.

Researchers

38. Determining the legal status of researchers involves distinct considerations:

a) **Controller** – Researchers will usually determine the "how and why" of their research projects. Therefore, it is likely that researchers will be controllers when processing DSO data for research purposes.

b) **Joint controller** – Researchers should be mindful that their relationship with the DSOs may result in them being joint controllers with the DSOs. The key to the determination of joint controllership is whether the entities decide the purposes and means of processing together. The indicators of when a joint controller relationship between DSOs and researchers may arise include (a) the degree of influence that a DSO has over the research, such as whether the DSO can dictate the terms of any research, its objectives or designing the processing operation in collaboration with the researcher, and (b) the benefit to be gained by the DSO (contrasted to the wider benefits to society from research). Thus, a genuinely collaborative research project, where DSOs and researchers decide questions jointly and share data and research findings both ways, will likely give rise to joint controllership of the research processing. When a joint controller relationship arises, this will in turn trigger further obligations on both parties. For example, the parties would have to enter into agreements as to their respective roles.

c) **Processor** – Researchers may act as processors, but in this context this will be a rare occurrence. One example would be where a DSO contracts researchers to conduct research on its behalf and then makes the data available to them. Where a researcher is simply working for a DSO, there will be no data sharing outside of the DSO organisation and therefore this Code will not be engaged. More commonly researchers will engage processors on their own behalf to assist in research processing, outsourcing (or even crowdsourcing) data analysis. In this case researchers must consider their obligations regarding that processor relationship (see paras 31 - 33 above).

Consequences of status

39. Where a joint controller relationship arises, the GDPR requires that the parties enter an arrangement reflecting their respective roles. For the purposes of this Code, that arrangement should be in writing, demarcating the processing activities for which they are responsible. That agreement must also reflect each party's obligations, in particular their respective responsibility in relation to the exercise of data subject rights under the GDPR.

40. If any party acts as a processor, the relevant controller must be satisfied that the processor offers sufficient guarantees that it will implement appropriate technical and organisational measures to meet the requirements of the GDPR. The controller and processor must have a written agreement in place governing that relationship. The GDPR is prescriptive about what should, as a minimum, be contained the agreement, including the subject matter and duration of the processing, nature and purpose of the processing, and type of personal data and categories of data subject. The agreement should also reflect the specific tasks and responsibilities of the processor in the context of the processing it is carrying out as well as the risk to the rights and freedoms of the data subjects and measures taken to safeguard and mitigate those risks.

41. DSOs and researchers should therefore determine which data sharing agreements will be required and put them in place before processing commences. In projects involving multiple research entities, this may necessitate a considerable number of agreements. This can be managed in one or both of the following ways:

    a) Entering into one data sharing agreement between the DSO and all researchers; and/or

    b) The DSO dealing directly with an independent third party, which stewards research data and enters into data sharing agreements with researchers; and/or

Liability

42. DSOs and researchers may face action from (i) supervisory authorities, other regulators and courts, or (ii) individual data subjects.

43. The parties should carefully consider the extent to which they genuinely need to be closely involved in each element of processing, as greater involvement increases the likelihood of joint controllership. DSOs can limit their involvement in determining the purposes and means of the research by (for example) not specifying research questions or research methodologies. This will help ensure that they are not deemed joint controllers (and therefore not liable) for the processing carried out by researchers.

44. The legal status that DSOs and researchers have will determine their liability. For most actions, the controller will be the primary actor responsible for compliance and consequent liability. However, the following aspects of the GDPR provide special arrangements that researchers and DSOs should be aware of.

Action for compensation

45. Article 82(1) GDPR provides that “any person” (i.e., not just a data subject but rather any natural or legal person) who has suffered “material” (e.g., a loss of money) or “non-material damage” (e.g., distress) can “receive compensation from the controller or processor for the damage suffered.”

46. Articles 82(4) of the GDPR provides for joint and several liability between multiple controllers, joint controllers and processors involved “in the same processing” for “any damage caused by processing” unless a controller or processor can show that they are not “in any way” responsible (Article 82(3)). This is a high threshold. Each controller and processor will be jointly and severally liable for “the entire damage” caused unless it is able to successfully raise this defence.

47. By way of mitigation, Article 82(5) provides that where a controller or processor has been required by a court to pay the entire amount of any compensation, they may reclaim monies from other controllers or processors to the extent of those

parties' responsibilities for the breach. However, this means that one party may be forced to make a payment of the entire amount of compensation and then seek repayment from the second party, even where the primary responsibility for the breach lies with the second party.

48. With Article 82(5) in mind, DSOs and researchers should use their data sharing agreement(s) to proactively clarify the extent of their responsibility for any processing in respect of which they are either joint controllers, or in a controller-to-processor relationship.

49. Finally, researchers and DSOs should consider Member States' implementation of the GDPR to determine the compensation regime(s) in the relevant jurisdiction(s). National and local regimes may differ on the right to compensation (refer to the compendium of Member State laws at Annex 4).

Non-monetary remedies

50. In addition to the right to seek compensation, data subjects may seek an "effective remedy" against a controller or processor where they consider their rights under the GDPR have been infringed. Such non-monetary remedies usually take the form of compliance orders, where a supervisory authority or a court orders a controller or processor to process data in a particular way or to stop processing data. That action will usually be directed at the controller yet the GDPR entitles data subjects to seek such orders against processors.

51. The GDPR allows data subjects to choose to bring such a case before either the courts where the controller or processor is based, or where data subjects have their "habitual residence". As such, data subjects have some flexibility in determining the applicable jurisdiction for their claim no matter where the main establishment of a controller may be.

52. In a DSO-to-researcher context, this may mean that proceedings are brought (i) where the DSO is based (ii) where the researcher is based and/or (iii) where the data subjects have their "habitual residence". Identifying where all data subjects

whose personal data is contained in the DSO or the research data are "habitually resident" should not be attempted, as it would contradict the principle of data minimisation. However, DSOs and researchers should assist each other by being transparent about their own jurisdictional considerations. This may be recorded in the data sharing agreement.

Action by supervisory authorities

53. Supervisory authorities are geographically based, with, at least one authority in each Member State. The rules on what action can be taken by supervisory authorities are complex and beyond the scope of the Code. However, researchers and DSOs should note that a supervisory authority can take enforcement action which may include audits of processing activities or administrative fines.

54. If controller(s) or processor(s) subject to the regulatory action are based in more than one Member State, the lead supervisory authority will usually be the authority in the Member State where the controller or processor has its main or single establishment, unless a complaint is lodged with an authority that relates only to an establishment or data subjects in that authority's Member State.

Section 3: Legal Bases for Processing

3A - DSOs and researchers must identify and record their legal basis for each processing activity they will engage in before processing data.

3B - Further processing of data by DSOs for qualifying research purposes will be compatible with their initial processing purpose pursuant to Article 5(1)(b) GDPR. Thus, if DSOs have an appropriate legal basis for their primary processing activities, they will not need an additional legal basis for sharing data with researchers.

3C - Researchers must identify a legal basis for their processing activities. The most suitable legal bases for researchers are Article 6(1)(f) GDPR, legitimate interests, or Article 6(1)(e), processing in the public interest.

3D - Where a research project seeks to rely on consent of data subjects as its legal basis for processing data, DSOs may assist researchers with obtaining the freely given, specific, informed and unambiguous indications of the data subjects' wishes. The DSO must facilitate the data subjects' conditions on consent, such as ease of withdrawal.

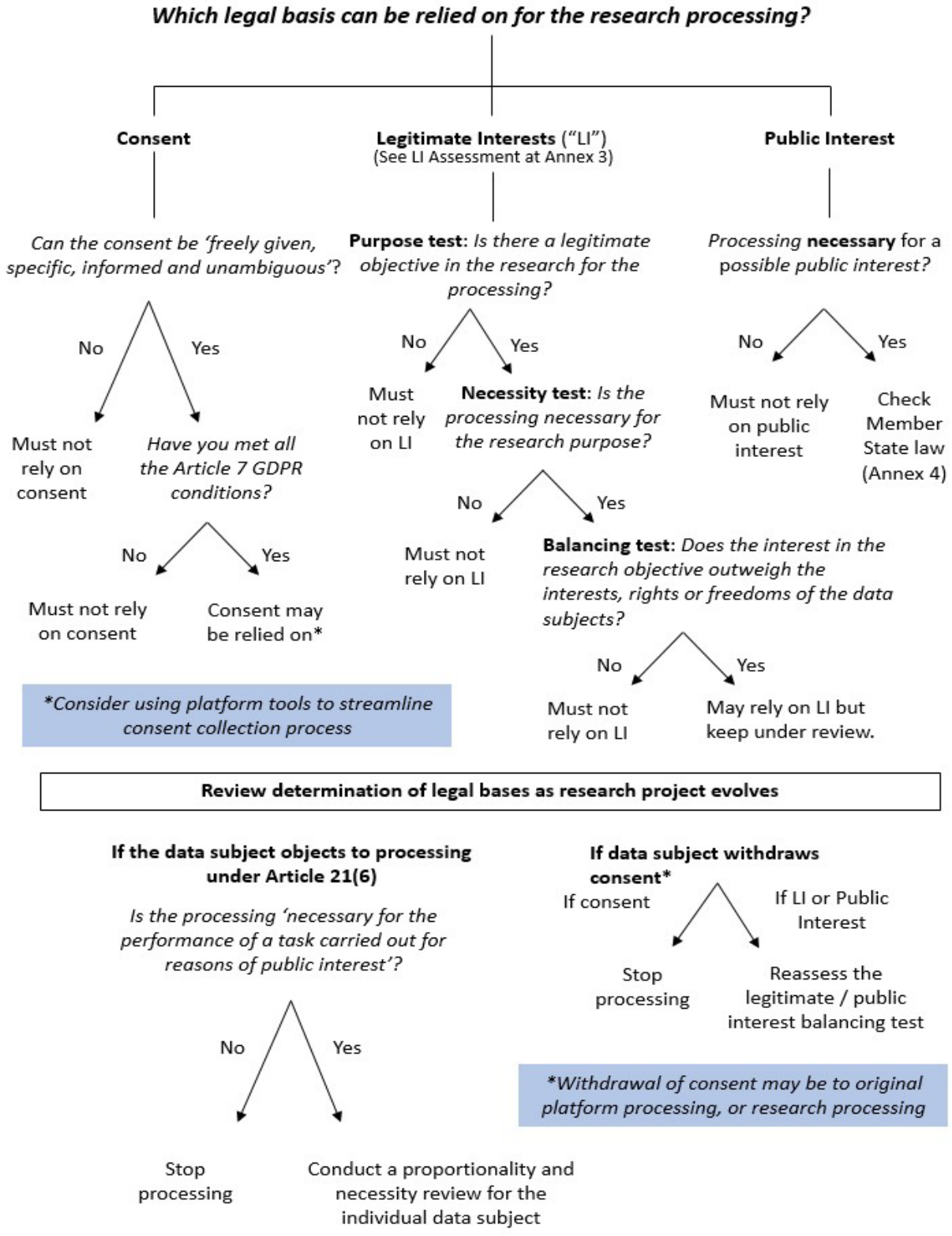
3E - DSOs and researchers must be mindful of enhanced protections for special category data and must only process special category data for research in accordance with a valid exemption and with specific measures in place to safeguard the fundamental rights and interests of data subjects.

Explanatory Notes to Section 3

55. The first data protection principle, in Article 5(1)(a) GDPR, requires data to be processed "lawfully". A controller must identify a lawful basis in Article 6 for each processing activity it undertakes. The processing operations of DSOs and researchers must be disaggregated to ensure the correct legal basis can be identified and justified. For instance, it is likely that DSOs will make data available while researchers will retrieve the data, thus generating two separate acts of processing recognised in the GDPR. DSOs and researchers must map the

processing activities required for a research project and identify and record their lawful basis for each processing activity before processing the data. Researchers and DSOs should be transparent with each other about their legal bases for processing and update each other if those bases are modified.

56. Clear identification of each controller's legal basis for each processing activity will also help DSOs and researchers comply with transparency obligations and protect data subject rights (see Section 5).


Which legal basis can be relied on for the research processing?
Consent
Legitimate Interests ("LI")
(See LI Assessment at Annex 3)
Public Interest
Can the consent be 'freely given, specific, informed and unambiguous'?
No
Yes
Must not rely on consent
Have you met all the Article 7 GDPR conditions?
No
Yes
Must not rely on consent
Consent may be relied on*
Purpose test: Is there a legitimate objective in the research for the processing?
No
Yes
Must not rely on LI
Necessity test: Is the processing necessary for the research purpose?
No
Yes
Must not rely on LI
Balancing test: Does the interest in the research objective outweigh the interests, rights or freedoms of the data subjects?
No
Yes
Must not rely on LI
May rely on LI but keep under review.
Processing necessary for a possible public interest?
No
Yes
Must not rely on public interest
Check Member State law (Annex 4)
*Consider using platform tools to streamline consent collection process
Review determination of legal bases as research project evolves
If the data subject objects to processing under Article 21(6)
Is the processing 'necessary for the performance of a task carried out for reasons of public interest'?
No
Yes
Stop processing
Conduct a proportionality and necessity review for the individual data subject
If data subject withdraws consent*
If consent
If LI or Public Interest
Stop processing
Reassess the legitimate / public interest balancing test
*Withdrawal of consent may be to original platform processing, or research processing

DSOs

57. DSOs' sharing of data with researchers will likely entail further processing for new purposes beyond their core purposes for processing data. It will therefore require fresh consideration of the legal basis for this processing.

58. Article 5(1)(b) provides that

> *further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.*

59. Therefore, there is a "presumption of compatibility" between the initial purpose of data collection and further processing of personal data for research purposes (see Section 1).

60. Where further processing is "compatible" with the initial purpose of data collection, Article 6(4) allows for further processing to rely on the same legal basis. As Recital 50 states, "*no legal basis separate from that which allowed the collection of the personal data is required*." Moreover, Recital 50 clarifies that further processing for research purposes "*should be considered to be compatible lawful processing operations*."

61. Thus, DSOs do not need a separate legal basis for sharing data with researchers, as such processing will be for a compatible secondary purpose. However, DSOs must be mindful of whether adequate safeguards have been implemented by the intended recipient(s) of the data (see Section 4).

Researchers[11]

62. Researchers must ensure they have their own legal basis for processing. The most relevant bases for researchers are legitimate interests (Article 6(1)(f)), public interest (Article 6(1)(e)), and, in limited circumstances, consent (Article 6(1)(a)).

Legitimate interests

63. Article 6(1)(f) provides that controllers may process personal data when

> *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.*

64. Researchers that rely on this legal basis should carry out and document a legitimate interests assessment before commencing processing. There is no standard format for this assessment, but it is important to record the reasons for the decisions taken. A template legitimate interests assessment is provided at Annex 3.

65. The constituent elements of the legitimate interests legal basis can be broken into three parts:

[11] The GDPR is unclear as to whether third parties such as researchers benefit from the relaxed rules on "further processing" for research purposes, such that a new legal basis for processing is not required. The European Data Protection Supervisor has suggested that the "compatibility presumption" can be relied on "by the original or a new controller". Others disagree. The European Data Protection Board has not addressed the issue in their guidance to date but dedicated guidance about further processing is expected to be released soon. See, The EU General Data Protection Regulation: A Commentary. Update of selected articles, covering developments between 1 August 2019 and 1 January 2021 (at page 76). See also, Becker et al, COVID-19 Research: Navigating the European General Data Protection Regulation J Med Internet Res. 2020 Aug; 22(8): e19799 (citing Dove ES. The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era J Law Med Ethics.

a) **Purpose test** – is there a legitimate objective in the research for the processing? What does that objective seek to achieve? Is the research focussed on the functioning of the DSO or on how users behave on the DSO? If so, there is likely to be a legitimate objective for the processing.

b) **Necessity test** – is the processing necessary for the research purpose, or could the same research objectives be achieved without processing personal data or with less personal data? It may not be possible to determine the outcome of the necessity test at the outset, particularly in exploratory research. However, the necessity of the processing should be kept under review.

c) **Balancing test** – is the interest in the research objective outweighed by the interests, rights or freedoms of the data subjects?

66. The GDPR does not provide an exhaustive list of processing scenarios that are by default in the legitimate interests of a controller or a third party, such that research is automatically designated as fulfilling a "legitimate interest". Rather, the determination of legitimate interests depends on the facts of a given processing operation.

67. To rely on the legitimate interests legal basis, controllers must balance their interests against the interests of the data subjects. In practice, this means researchers must assess the specific processing involved in each project against the impact that their research would have on data subjects, including the "*interests or fundamental rights and freedoms of the data subject*". Researchers should note that where data subjects are children the balance is in favour of the rights of the children over the objectives of the processing. This balancing exercise should be documented and made available to supervisory authorities and regulators upon request.

68. Recital 157 identifies the benefits associated with research using personal data, including the potential for new knowledge about "*widespread medical conditions*"

and the "*long-term correlation of a number of social conditions*." Further, the results of research can "*provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people, and improve the efficiency of social services*." Any balancing exercise may refer to these benefits (to the extent they apply to the specific project) expressly identified by the GDPR.

Public interest

69. Where the objectives of research benefit the public interest, the legal basis of a "task performed in the public interest" in Article 6(1)(e) *may* have utility for researchers. This approach is supported by European regulatory authorities. For example, the EDPB has stated that public interest is more appropriate as a legal basis than consent for research in clinical trials. Researchers should not assume, however, that their work will *automatically* engage this lawful basis, even if they believe it to be broadly in the public interest.

70. The availability of the public interest legal basis must be established by Union or Member State law. Researchers must therefore demonstrate they meet the requirements to use this lawful basis by reference to either (i) the domestic law in their jurisdiction or (ii) EU law. Researchers should refer to the compendium of Member State laws provided at Annex 4 as part of this assessment.

Consent

71. For certain research projects, researchers may rely on the consent of data subjects. Consent has a high threshold, as data subjects must provide "specific, informed and unambiguous" indication of their wishes. This is a particularly strong constraint in a research context and may limit the utility of this legal basis. As Recital 33 GDPR recognises, it is

often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

72. However, consent may be an appropriate legal basis in certain projects that have clear research aims that can be communicated to data subjects at the outset and are unlikely to change. In these circumstances, DSOs should work with researchers to ensure consent is properly obtained, such that the consent is specific, informed and unambiguous.

73. DSOs should also assist researchers in meeting the conditions on consent. Those conditions are:

    a) The controller is to demonstrate that the data subject consented.

    b) If consent is sought in writing, consent for the specific processing purpose must be distinguishable from other matters within the written document.

    c) The data subject should be able to withdraw consent as easily as they provided consent.

    d) The provision of a service cannot be conditional on consent.

74. DSOs may be able to meet these conditions using the features built into their product.

75. The applicability and appropriateness of a legal basis for processing should be kept under review. Researchers should review their determination of their legal bases as their research project evolves. DSOs must inform a researcher if a data

subject exercises rights in a way that may impact the researcher. For example, if the DSO were relying on consent, an individual may exercise their right to withdraw that consent. The withdrawal of consent could, in turn, impact the legitimate interest assessment conducted by the researcher as the expressed desire of the data subject to no longer have their data processed will have to be weighed by the researcher against the interests in the continued research (although it would not automatically require the researcher to cease processing).

Necessity and relationship to purposes of processing

76. The analysis of the controller's legal basis will require consideration of the purpose of the processing, the necessity of the processing to achieve those objectives and the context in which the processing occurs.

77. In five of the six grounds for processing data in Article 6 GDPR, the processing must be "necessary" for the specified purposes. Necessity asks whether the same means can be achieved by less intrusive methods. Where a controller relies on a legal basis that requires a test of necessity such as legitimate interests in Article 6(1)(f), the controller will therefore have to demonstrate that the processing is required for their purposes to be functional.

78. In a research context, the researcher will have to document why their research is not possible without processing the data. The researcher must have a specific purpose for which they need the data that relates to the needs of a research project. If that research objective can be achieved without the personal data, the necessity test will not be met.

79. Researchers should consider what data are required to answer their specific research question(s). For instance, is the purpose of the research to understand the actions of individuals on a DSO or the conduct of the DSO itself? If the focus is the DSO, the researcher should consider what personal data are required to conduct research on the DSO. While it may not be possible to fully appreciate

what data are required at the outset of a project, particularly in exploratory research, the necessity of processing data should be kept under review.

80. DSOs should consider how broad datasets can be prepared and made available to maximise the scope of potential research. Individual decisions can then be made about which specific researchers or research projects are able to access which variables, based on the identified data requirements of their research question(s), thus reconciling the aim of facilitating research with the principles of necessity, purpose limitation and data minimisation.

81. If the necessity test can be met, researchers must be mindful to not process the data in a way that is incompatible with that purpose.

Special category data

82. Under the GDPR the processing of special category data is prohibited. The special categories of data are listed in Article 9(1) as follows:

> *Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*

83. The prohibition in Article 9 extends to:

a) Processing "revealing" racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. For the purposes of this Code any processing revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership should be regarded as engaging Article 9, regardless of the controller's intention. For example, if a researcher combines various datasets in a way that means inferences can be drawn about an individual's political opinion, irrespective of whether that is the intention of the researcher,

such processing would engage Article 9 GDPR. It is unclear under the GDPR if the data processed must accurately reflect a relevant Article 9 trait. However, for the purposes of this Code DSOs and researchers should assume that accuracy is an irrelevant consideration.

b) Processing to "uniquely identify" an individual by genetic data or biometric data. However, this is relatively unlikely to be relevant in the context of qualifying research for the Code.

84. Processing of special category data is prohibited unless the data controller can rely on one or more of the grounds listed in Article 9(2) GDPR. The most relevant of those grounds to DSOs and researchers are discussed below.

Considerations for DSOs and researchers

85. There are three issues for consideration for DSOs and researchers:

a) The "presumption of compatibility" for Article 6 data (i.e., that processing which is compatible with the initial purpose of collecting data will not require a new legal basis for processing) does not extend to processing for a secondary purpose that engages Article 9. Thus, where a DSO's processing for research under this Code engages Article 9, an exemption permitting such processing will be required under that Article. DSOs should be cognizant that even where their core processing does not engage article 9, new and different processing for research purposes may do, for example where such processing involves the new combination of previously siloed datasets with the effect of 'revealing' the relevant characteristics.

b) Article 9(2)(j) provides that special category personal data may be processed where the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The processing must also be (i) in accordance with Article 89(1) and (ii) based on Union or domestic laws.

i) Article 89(1) GDPR requires (i) safeguards that address the rights and freedoms of data subjects, and (ii) that technical and organisational measures are in place. The right combination of safeguards will depend on the risks involved in each research project. Whilst the GDPR expressly refers to data minimisation, as well as citing pseudonymisation as an appropriate technique, many other approaches are available and may be appropriate. Section 4 and Part II of this Code can be used as a guide to reach a pragmatic decision on which safeguards to put in place for a particular piece of research, based on the risks involved.

ii) Union or Member State law is required to use this provision. In the absence of Union law authorising the processing, DSOs and researchers will have to refer to domestic law. The DSOs (to the extent they require a new Article 9 exemption) and researchers will have to consider the laws in their Member State (or place of main establishment). To assist DSOs and researchers with understanding and appreciating their own member state laws, a compendium of select Member State laws is at Annex 4.

c) Article 9(2)(e) provides an exemption where processing is of special category data that has been manifestly made public by a data subject. The phrase “manifestly made public” is not defined in the GDPR and has not been consistently interpreted. Most approaches require the data subject to have made the data universally accessible in practice and made public by a volitional act of the data subject. Data disclosed via a public profile on a closed DSO is not necessarily “manifestly made public”. Thus, while this exemption may be relevant to some research projects, data being “manifestly made public” by a data subject is a high standard which would be unlikely to be met where Article 9 traits are revealed or inferred by processing.

86. Thus, DSOs and researchers must consider whether special category data will be processed as part of the research project. They should identify which specific processing activities will use special category data, and which actors are controllers in respect of that processing. Finally, considering any existing exemptions for that processing on which DSOs may rely, they should identify which exemption(s) each controller will rely on at each stage of the process. These determinations should be made in advance, but DSOs and researchers should be cognisant that the data processing involved in a project evolves over time, such to impact the processing of special category data (for example, if objectives change or if new characteristics of a dataset come to light).

Overlap between Article 6 and Article 9 GDPR

87. DSOs and researchers should note the interaction between Articles 6 and 9:

a) Any processing of personal data will need to be justified by reference to Article 6 GDPR.

b) To lawfully process special category data, the controller must identify a lawful basis under Article 6 and an exemption under Article 9. These do not have to be linked (e.g., a researcher may rely on its legitimate interests for the research, and the public interest exemption to the extent the research requires special category data to be processed).

Section 4: Security and Safeguards

4A - DSOs and researchers must process data securely, with appropriate technical and organisational measures in place, and only use data processors that can show they also have appropriate technical and organisational measures in place.

4B - The security measures must be appropriate to the nature, scope, context and purpose of the processing involved in the research, and the risks posed to the rights and freedoms of individuals. They must be incorporated by DSOs and researchers as binding and enforceable commitments through data sharing agreements.

4C - The security measures used must comply with the "data protection by design and default" approach, including limiting processing to that necessary to achieve the research objectives.

4D - DSOs and researchers must assess risks and agree appropriate security measures in good faith, taking account of the benefits of research and preventing security requirements from unduly preventing or impairing it.

Explanatory Notes to Section 4

88. The sixth data protection principle ('integrity and confidentiality') contained in Article 5(1)(f) GDPR requires data to be processed securely. This means data must be processed in a manner that ensures "*appropriate security of the personal data*". The GDPR also expressly refers to the need to safeguard personal data (and data subjects' rights and freedoms) in the context of research to be able to rely on the research exemptions (Article 89). Among other things, the GDPR requires the use "*appropriate technical or organisational measures*" in data processing as part of these safeguards.

89. There is no exhaustive definition of what constitutes a technical or organisational measure. Technical measures include those relating to technology, hardware and software used, but also access controls, logs, and cybersecurity. Organisational measures include provisions for where responsibility lies between

and within organisations, including by whom and how frequently issues are reviewed and assessed. **Part II of this Code provides guidance for researchers and DSOs as to technical and organisational measures that may be appropriate as safeguards, highlighting the state of the art and best practices.** These practices will need to be tailored and adapted to the need, scope, and structure of the DSOs and researchers involved.

90. Risk assessment and mitigation should not be used to unduly frustrate or impair the research. DSOs and researchers should work together in good faith to identify pragmatic solutions that take into account the benefits of the research being facilitated. Where the DSOs and researchers cannot reach agreement on the security measures to be implemented, they may consider referring their proposed risk management arrangements to an independent third party with expertise in the processing of personal data for research.

DSOs

91. DSOs will have a primary purpose for the processing of personal data which is the subject of interest to researchers. Sharing data for research purposes will be a *secondary* purpose for DSOs. DSOs must therefore implement technical and organisational measures to ensure security of processing and safeguards of individual rights for that secondary purpose.

92. Before making personal data available to researchers, whether through a secure operating environment or otherwise, DSOs should ensure that there are appropriate technical and organisational security arrangements in place regarding the access and sharing of data.

Researchers

93. Researchers must consider what measures they may need to implement to ensure the data is processed securely, such as guaranteeing their own staff confidentiality, secure operating systems, and other steps to identify and mitigate potential risks arising from the research.

94. Processing only the data that is *necessary* to achieve the research purpose is a non-technical safeguard. Researchers must therefore consider at the outset what data processing is truly necessary to promote the objectives of the research. If the objective of the project means that personal data are required, researchers should consider measures such as anonymisation of the data (if anonymisation is possible). Alternatively, researchers should consider whether the data can be pseudonymised and if so, what steps against re-identification can be implemented to protect data subjects.

95. Further, researchers should have systems in place to ensure an adequate level of control over how data are used to ensure that the data shared with them by DSOs under this Code are used only for purposes linked to the original research objectives.

96. When considering the adequacy of security and safeguards in place, researchers should have due regard for the mechanisms used to transfer data. For example, a DSO may maintain a secure operating environment in which the researchers may process the personal data which has been disclosed to them. In such cases, the researchers should comply with the requirements of the secure operating environment operated by the DSO. Compliance with those steps will not negate the need for researchers to have additional security measures and safeguards in place for their own processing activities.

DSOs and researchers

97. To facilitate access to data for research purposes, DSOs and researchers should work together to (i) map the processing involved in the research project and (ii) ensure that appropriate security measures are in place for each processing activity involved. In some cases, it will be appropriate for this exercise to result in a full data protection impact assessment. The EDPB have adopted guidelines on high-risk processing that provide guidance on when this might be the case.

Processors

98. If a third party were to process data on instructions from and on behalf of a researcher or DSO, that third party may be a data processor. Where a data processor is being used, further considerations arise under Article 28 GDPR. Importantly, DSOs and researchers must ensure that they only use processors that can *"show they have appropriate technical and organisational measures in place".* To comply with this requirement, DSOs and researchers should be able to understand the measures the processor has in place and to audit the adequacy of those mechanisms. For researchers this will be of particular relevance when using outsourced data processing services or crowd-sourcing approaches.

Understanding the risks

99. Security measures must be "appropriate" to the nature and purpose of the processing and risks posed to the rights and freedoms of individuals. That risk cannot be predetermined but must be assessed in relation to each processing activity.

100. DSOs and researchers should map the processing involved in their research and assess and document the risk(s) associated at the outset (as part of a data protection impact assessment if appropriate). This must include consideration of the nature of the personal data that will be processed, including whether any special category (or otherwise sensitive) data will be processed. The risk factors within Part II of this Code can be used to analyse the risks within the research project and the measures deployed to mitigate them.

Typical risks arising in the DSO to researcher context

101. Risks explicitly recognised by the GDPR pertain to confidentiality (unauthorised access or disclosure), integrity (unlawful or accidental alteration) and availability (accidental or unlawful destruction). Consideration must also be given to risks that may lead to "physical, material or non-material damage" and risks to the

rights and freedoms of natural persons. This could, for instance, include the risk of discrimination from the proposed processing activity.

102. Part II of this Code contains guidance regarding the common risks that arise in a DSO-to-researcher data sharing context, which may assist DSOs and researchers with conducting their risk assessment.

Implementing measures to mitigate risk

103. It is not possible to prescriptively or exhaustively define a set of security measures that can be applied in all cases of DSO-to-researcher data sharing. Considerations of which security measures will be appropriate will vary depending on the research project and the data processing involved. Measures that should be considered include procedures for mutual notification of data breaches and techniques which comply with the principle of data minimisation such as pseudonymisation and encryption of personal data, and with that of limited storage periods.

104. Part II of this Code sets out how these common techniques, and others, work in practice and highlights some best practice examples that are useful in a research context. In selecting appropriate measures, DSOs and researchers should consider the range of security measures available to them, reflecting industry best practice and the costs of implementation when deciding what measures are appropriate for a particular research project.

105. Any agreed measures must cover the entire processing lifecycle up to erasure. DSOs and researchers should record the rationale behind the measures chosen and any residual risks they accept as part of the research in their data sharing agreement.

106. DSOs and researchers must incorporate the agreed set of security standards into their data sharing agreement as binding and enforceable commitments. This will also enable the parties to rely on the Code, together with the data sharing

agreement, as a third-country transfer mechanism pursuant to Article 46(2)(e) GDPR.

107. DSOs and researchers must implement the agreed-on standards in their processing.

108. DSOs and researchers should agree on a process for ongoing monitoring, review and improvement of the security standards and incorporate these provisions in their data sharing agreement. They may consider the involvement of a third-party body with expertise in the use of personal data for scientific research to monitor the implementation of their security arrangements.

109. Having strong technical and organisational measures will also assist in demonstrating compliance with the principle of "data protection by design and default". That principle means that security measures that have been implemented must be kept under review to ensure they are suitable and appropriate to the risks, as well considering wider principles such as retention periods and the continued necessity of processing the data (see Section 3) and processes for deletion and return of data. Technical and organisational security measures must therefore be implemented from the earliest stages of a research project and throughout its lifecycle.

Section 5: Transparency and Data Subjects' Rights

5A – DSOs and researchers must assess the level of transparency required for their processing activities, and the rights of data subjects that will apply to the processing they will carry out.

5B – DSOs and researchers must enter into binding commitments to implement appropriate measures that provide transparency about the data processing carried out under this Code.

5C – DSOs and researchers must enter into binding commitments to implement measures that give data subjects sufficient scope to exercise their GDPR rights, taking into account the nature of the research and any applicable exemptions or derogations.

5D – DSOs and researchers must record the rationale for the arrangements they put in place, including which research exemptions they are relying on (if any).

5E – DSOs and researchers must keep each other informed about the exercise of data subject rights relevant to research carried out under this Code.

Explanatory Notes to Section 5

Transparency

110. The first data protection principle in Article 5(1)(a) GDPR requires data to be processed transparently. The burden for compliance falls on controllers, who must "take appropriate measures" to inform data subjects of the nature of the processing activities and the rights available to them "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".

111. The GDPR provides specific modalities of transparency, which differ depending on whether the data is collected (a) directly or (b) indirectly from the data subject. Some of the requirements overlap but differ in ways that are particularly relevant to the DSO-to-researcher context.

a) **Article 13 GDPR** – Controllers are required to provide a range of information before processing data when collecting data directly from data subjects. This includes specific information about the "*purposes for which the personal data are intended as well as the legal basis for the processing*". If a controller intends to process data for a further purpose, the controller is required to inform data subjects about that further processing but the controller will not be required to provide the full suite of information. Article 13(3) GDPR specifies that the information to be provided for further processing must include information on such further purpose and any relevant information from Article 13(2) which mainly relates to data subjects' rights.

b) Article 14 GDPR – If the data are not collected directly from data subjects, then there are certain exemptions to the requirement to provide information to the individuals. Of relevance in a DSO-to-researcher context are exemptions from transparency requirements where disclosure (i) is not necessary because the individual already has the information, (ii) proves impossible, (iii) involves a disproportionate effort, or (iv) is likely to render impossible or seriously impair the achievement of the objectives of that processing: These are discussed in more detail at para 121 below.

112. This means that DSOs and researchers will often have independent and differing transparency requirements to meet in respect of their different processing operations, from the DSO's core processing through to sharing data and processing by researchers for qualifying research.

113. DSOs and researchers should provide information in a transparent and precise manner without restricting avenues for future research at the point of data collection. DSOs should not use unduly restrictive interpretations of the requirement for transparency to either prevent or frustrate the aims of research. The appointment of dedicated teams to facilitate research (pursuant to Clause

1H of this Code) would promote balanced, consistent, and pragmatic solutions to providing transparency.

DSOs

114. DSOs collect data directly from data subjects for their primary processing purposes. As such, DSOs should have mechanisms to satisfy their transparency obligations. Typically, this information will be provided in DSOs' main privacy notice.

Modalities of transparency

115. In most cases, the DSO data of interest to researchers will have been collected for the DSO's primary purposes. Facilitating research will be a secondary purpose of processing. Qualifying research is recognised as a compatible secondary purpose (see Section 3), but information must be provided on secondary processing purposes to enable data subjects to understand how their information is being used. As such,

    a) DSOs should not rely on broad statements such as "we may use your personal data for research purposes" in their main privacy notice. They should provide more clarity and specificity about the way personal data will be used.

    b) DSOs should however avoid impairing the research objective. To this end, providing too much information to individuals who are subject to the research may result in those individuals modifying their behaviour or otherwise impairing the research.

    c) DSOs may not know at the time of collecting data the precise research purposes for which that data may later be processed. They will need to provide information that is sufficiently specific without unduly and irreversibly closing off potential future avenues of research at the point of data collection.

116. In sum, there is a balance to be struck. Potential solutions may include:

    a) DSOs could create a dedicated page (whether separately, jointly, or via a funded third party) which lists the research projects where data has been shared. The level of detail provided would be balanced against the impact on the research project, and DSOs and researchers would need to work closely together to strike the right balance. Thus, where providing granular detail – such as specific information on the institution conducting the research or what the project's proposed focus is or the potential outcomes – would impair the research, DSOs could provide high-level explanations as to why that data was shared for the project. Ideally, the level of detail to be provided should be agreed between the DSO and researchers prior to notice of that specific research project being provided to users. That page referring to the research should be referenced and directly linked in the main privacy notice used by the DSO. Data subjects could be alerted to this new section of the website by way of a one-time pop-up message. Data subjects should be able to consult this research page at any time and use it to exercise their rights.

    b) An independent third party could host details of data sharing between DSOs and researchers. That third party would work with researchers and DSOs to determine what level of detail is appropriate to provide to individual data subjects. Individual data subjects could then make enquiries directly with the third party. The DSOs could then refer to that third party in their transparency notice.

117. DSOs should record the reasons for the decisions they have taken about what information to provide in transparency notices.

118. As it may not be possibly to fully specify research purposes in all cases, it will be imperative to ensure that data subject rights can be exercised easily in relation to the processing. This will introduce an important safeguard, especially in circumstances where full transparency cannot always be guaranteed.

Researchers

119. Researchers are unlikely to have a direct relationship with the data subjects. Instead, researchers will likely receive data indirectly from DSOs. In this case, transparency obligations are subject to exemptions which are of direct relevance to researchers.

120. The basic obligations are contained in Article 14 GDPR, which provides that data subjects must be informed of matters such as the identity of the data controller, the purposes of the processing and related legal bases and the categories of personal data concerned. Article 14(2) further requires information to be provided on individual rights and retention periods. The information is to be provided at the latest within one month of receiving the personal data, subject to the exemptions set out below.

Research exemptions to providing transparency information

121. These obligations do not arise if such transparency would (i) be impossible (ii) involve disproportionate effort or (iii) render impossible or seriously impair the achievement of the objectives of that processing:

a) **Impossible** – Practically, impossibility is a high threshold. As such, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide this information to data subjects.

b) **Disproportionate effort** – Researchers should consider the number of data subjects, the age of the data and any appropriate safeguards adopted. Researchers could for example rely on the disproportionate effort exemption where the data from a DSO involves numerous data subjects, or where it would be difficult to reidentify data subjects from a pseudonymised dataset for contact purposes.

c) **Render impossible / seriously impair the research** – This ground is of most utility to researchers. The researchers will have to weigh the

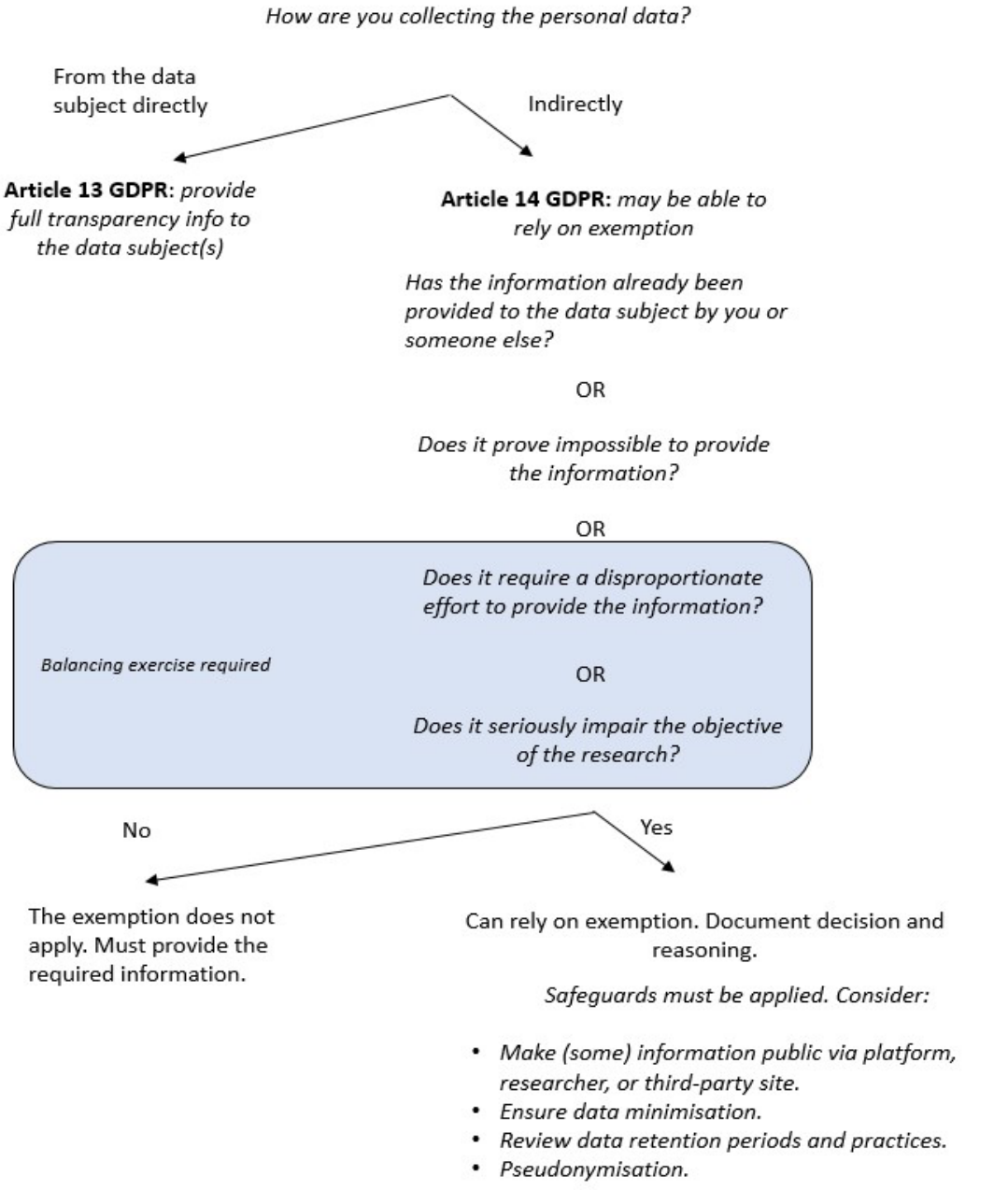
impact of transparency on the research. If complying with the transparency requirements will "render impossible" (i.e., mean that the research cannot progress) or "seriously impair" (i.e., impact the research objectives), then the researcher may reduce the amount of information made available to data subjects. For example, data subjects might modify their behaviour because they know their behaviour is being analysed, or transparency information might alert groups hostile to the research aims and encourage or enable them to disrupt it.

122. The researcher must record their decision-making leading to reliance on these exemptions. If researchers rely on one of them, they must implement appropriate measures to protect the data subject's rights, freedoms, and legitimate interests. As a starting point this will include making the transparency information required by Article 14 public. Researchers should then assess whether any transparency information should not be made public on the basis that it would render impossible or seriously impair the research.

123. Other safeguards may include ensuring data minimisation, clear and operational retention periods and/or pseudonymisation.

124. The transparency requirements also do not arise where the individual already has the information. In a DSO-to-research context, this may arise where the individual has received the information directly from the DSO. Whether the individual has already been provided with the information will need to be assessed on the facts. However, as a DSO has limited transparency obligations for further use of data such as data sharing with researchers it is unlikely that the data subjects will have detailed information such that the researcher's own transparency obligations are completely negated.

Can researchers rely on an exemption from providing transparency information to data subjects?



Modalities of transparency

125. As a data controller, the researcher is required to demonstrate compliance with the transparency requirements unless an exemption applies. The clearest method of ensuring compliance is to provide the information directly to data subjects (though this may be difficult in practice). If they rely on an exemption, researchers should make the Article 14 information public on their own project website, without publishing information that would render impossible or seriously impair the research.

126. Alternatively, the researcher could request that the DSO provides this information to data subjects as part of the information the DSO makes available to data subjects about processing for research purposes, such as through the DSO's dedicated webpage. DSOs and researchers could alternatively seek to have the information hosted by an independent third party.

DSOs and researchers

127. Researchers and DSOs should work together to map the processing activities involved in the research and determine in advance the appropriate transparency measures for each element of processing. DSOs and researchers should consider seeking critical input from an expert independent body, particularly with regard to the modalities of transparency and to key decisions on whether transparency information is appropriate and whether information can be legitimately withheld from data subjects.

128. The agreed transparency measures should be recorded in binding and enforceable commitments between DSOs and researchers as part of the data sharing agreement.

Data Subjects' Rights

129. The rights of data subjects include the right to be informed (Articles 13 and 14), the right of access (Article 15), the right to rectification (Article 16), the right to erasure (Article 17), the right to restrict processing (Article 18), the right to data

portability (Article 20), the right to object (Article 21), and rights in relation to automated decision making and profiling (Article 22). Where a data subject makes a request to exercise their rights, the controller must respond as quickly as possible and at the latest within one month of receiving the request. Processors also have obligations in responding to data subject rights. For instance, processors are obliged to assist a controller with responding to the exercise of rights by data subjects. Further, some rights can be enforced directly against processors, such as the right to object.

130. Data subjects' rights vary in application depending on the lawful basis for the research processing. For example, the general right to object in Article 21(1) GDPR arises where the lawful basis is public interest or legitimate interest. In the DSO-to-researcher context, each entity may have different lawful bases for different processing activities. Where DSOs and researchers rely on separate lawful bases, the rights that attach to the processing may differ. This may create a situation where the DSO faces an objection request which means they must cease processing the individual's data, but the researcher can continue with its research processing (subject to a legitimate interest balancing exercise, for example). DSOs and researchers will therefore need to (i) understand their legal status and lawful bases for each processing activity (Sections 2 and 3], and (ii) implement processes that allow them to respond to (and communicate with each other about) the exercise of data subjects' rights, for example through the DSO's dedicated team (see Section 1) and the named individual(s) on the data needs and management plan (see Part II).

<u>Research exemptions to data subject rights</u>

131. There are some exceptions for data subject rights for processing related to research:

    a) There is an exemption from the right to erasure where the right would "render impossible" or "seriously impair" the achievement of the research purposes. The requirement is more than just an inconvenience or

difficulty in meeting the objectives of the research. In practice, this will require researchers to demonstrate that compliance with the right to erasure could undermine the statistical validity of processing which has already taken place or impact the integrity of their dataset. In such cases, researchers will be able to continue processing data for research despite the erasure request.

b) An individual can object to such processing, on grounds relating to his or her particular situation, unless the processing is necessary for performance of a public interest task. Thus, organisations relying on the public interest legal basis for their research processing will be exempt from objections to processing.

132. There may be further limitations on data subjects' rights to access, rectification, restriction, and the right to object where processing is for research purposes under Member State Law. A compendium of relevant domestic laws is included at Annex 4.

Considerations for DSOs and researchers

133. DSOs and researchers should work together in good faith to implement and document procedures for responding to the exercise of data subjects' rights, bearing in mind their respective legal bases for processing. The procedures should be flexible enough to deal with the fact that different data subjects may have different rights depending on their member state, but this does not mean that the member state of every data subject needs to be determined in advance. These procedures should be entered into as binding commitments as part of the data sharing agreement.

134. Whilst responding to data subject rights requests may be complex, it should not be permitted to unduly impair research. DSOs and researchers should negotiate appropriate arrangements in good faith, taking account of the value of the scientific research being facilitated. If agreement is difficult, they may consider

referring their proposed arrangements to an independent third party. Where a significant amount of complexity is anticipated (for example, where the project involves data subjects from multiple jurisdictions) DSOs and researchers might consider the utility of involving a third-party body capable of understanding and responding to the exercise of data subjects' rights in relation to the research processing.

135. In practice, the DSO will be the first point of contact for data subjects as it has a direct relationship with them. The DSO will already have policies and procedures in place for handling data subject rights requests in relation to their core processing, which can be repurposed as necessary for the research project.

136. If a DSO receives a valid data subject rights request that affects the legal basis for its primary processing (on which the DSO in turn relies for the processing of data shared with researchers), it must consider the wider consequences of the exercise of those rights:

    a) In the case of withdrawal of consent, that DSO must ensure it gives effect to that withdrawal of consent for any further sharing of data to researchers.

    b) In the case of an objection request where processing is based on legitimate interests, any controllers will need to revisit their legitimate interests assessments in light of the objection request to determine if they retain a "compelling" interest that override those of the data subject. The need to show compelling reasons suggests a higher threshold than would be required to justify processing as part of a legitimate interests assessment under Article 6. The burden on demonstrating "compelling" interests rests with the controller, which should retain a written record of the reasons for its decision.

137. Where the DSO receives a rights request from a data subject, it must advise the researcher of the request and of the outcome of its decision (such as if it has

decided to cease processing). This will enable the researcher to independently determine whether the exercise of rights by the data subject impacts the lawfulness of the researcher's own continued processing, taking into account matters such as the legal basis relied upon and the feasibility of identifying the data subject. For example, if a user objects to the DSO's primary processing this may impact the researcher's legitimate interest assessment. However, researchers are not obliged to follow the same course and must make their own assessments as to whether their continued processing is justified by their compelling interests. If a data subject makes a request to exercise their rights to the researchers directly, the researcher should likewise notify the DSO.

Identification of data subjects

138. Where a rights request is made to a DSO, identification of the data subject will be straightforward. Where datasets have been passed to researchers, however, data subjects' identities may be difficult to establish, for instance because the dataset may have been pseudonymised. Under Article 11 GDPR, researchers are not obliged to process additional information in order to enable the reidentification of data subjects.

139. In designing the procedures for data subjects to exercise their rights, therefore, DSOs and researchers do not need to provide for every individual to be capable of being reidentified by researchers.

Section 6: Jurisdiction & International Data Transfers

6A - DSOs and researchers must seek to ensure the protection of all personal data processed as part of their research, irrespective of considerations of jurisdiction and applicable law.

6B - DSOs and researchers must anticipate any transfers of personal data outside of the European Economic Area required for their research, and must ensure that an adequacy decision or documented and binding appropriate safeguards are in place before transferring data.

6C - DSOs and researchers must not export or import data to or from a country if they have any reason to believe that the third country's laws prevent them from fulfilling their obligations under the Code.

Explanatory Notes to Section 6

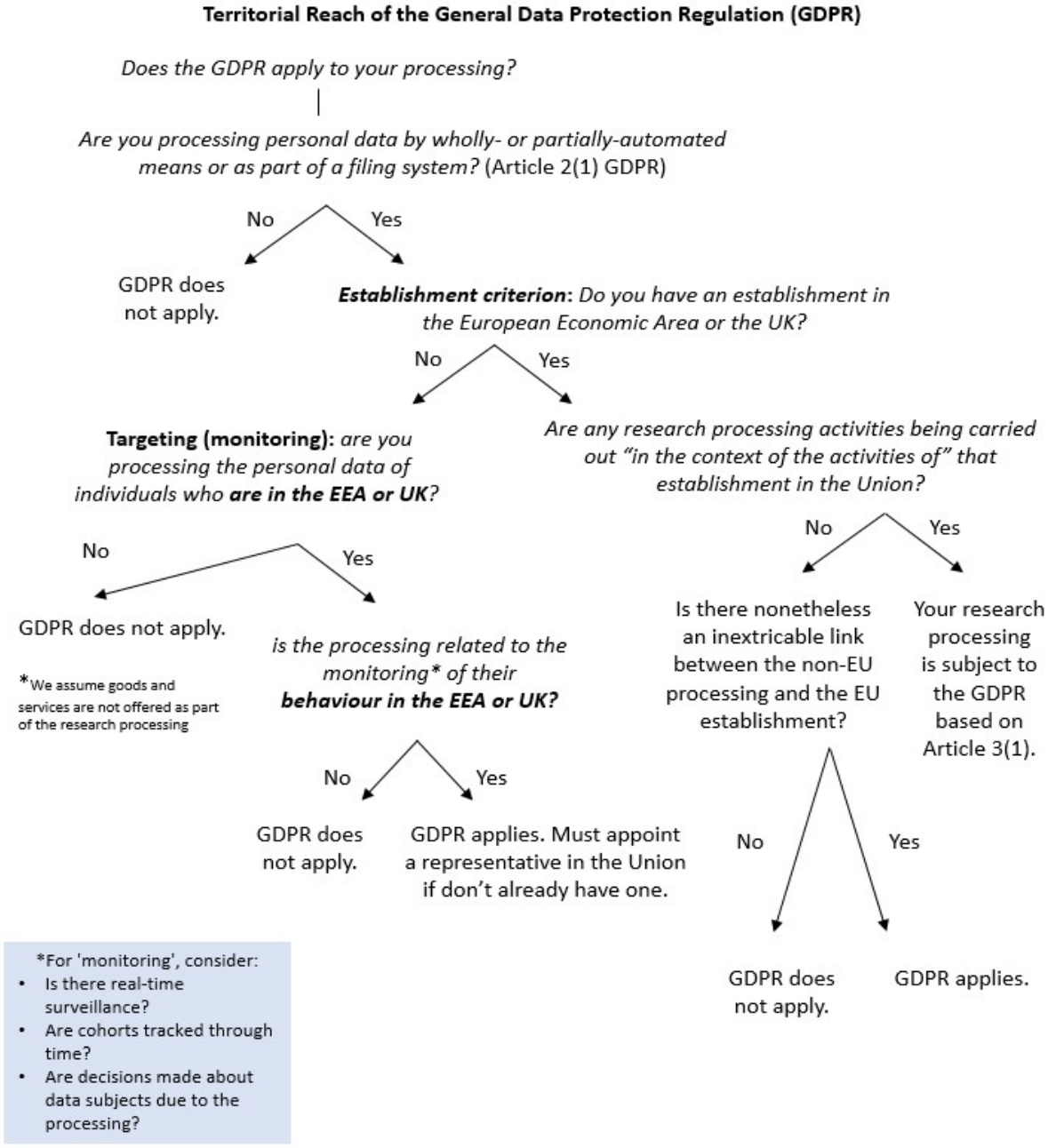
Territorial Application of the GDPR

140. Before sharing data with each other DSOs and researchers should each independently appraise the extent to which the GDPR applies to their research processing activities as they will have the best understanding of their own context.

141. A research processing activity will fall within the territorial scope of the GDPR:

    a) if the establishment criterion in Article 3(1) GDPR applies to the DSO or researcher, or

    b) if the targeting criterion in Article 3(2) GDPR applies to the DSO or researcher.


Territorial Reach of the General Data Protection Regulation (GDPR)
Does the GDPR apply to your processing?
Are you processing personal data by wholly- or partially-automated means or as part of a filing system? (Article 2(1) GDPR)
No
Yes
GDPR does not apply.
Establishment criterion: Do you have an establishment in the European Economic Area or the UK?
No
Yes
Targeting (monitoring): are you processing the personal data of individuals who are in the EEA or UK?
Are any research processing activities being carried out "in the context of the activities of" that establishment in the Union?
No
Yes
GDPR does not apply.
*We assume goods and services are not offered as part of the research processing
is the processing related to the monitoring* of their behaviour in the EEA or UK?
No
Yes
Is there nonetheless an inextricable link between the non-EU processing and the EU establishment?
Your research processing is subject to the GDPR based on Article 3(1).
No
Yes
GDPR does not apply.
GDPR applies. Must appoint a representative in the Union if don't already have one.
No
Yes
GDPR does not apply.
GDPR applies.
*For 'monitoring', consider:
• Is there real-time surveillance?
• Are cohorts tracked through time?
• Are decisions made about data subjects due to the processing?

Establishment criterion and associated considerations

142. Any real and effective activity, even minimal, through stable arrangements in the European Union can bring a controller, joint controller, or processor within scope of the GDPR. Even controllers, joint controllers, or processors that are based outside the Union can come within scope of the GDPR if the data processing activities are happening in the context of an establishment in the Union. For the purposes of the establishment criterion, it is not necessary that the processing take place in the EU or that the data subjects are located in the EU.

143. There are two questions to consider in order to assess whether such activities fall within scope of the GDPR.

144. **Firstly,** DSOs and researchers should each consider if they have any establishment(s) in the European Union:

    a) If a DSO or researcher has a branch, office, group company, agent, or other stable relationship within the Union then it will have an "establishment" (even a single employee could amount to an establishment if they are set up to work in the Union).

    b) DSOs and researchers should note that if they are joint controllers (see Section 2) they should consider if any of them has any establishments in the Union.

    c) If either a DSO or researcher engages a processor (or one of them acts as a processor for the other), the establishment of the processor will not constitute establishment for the controller.

145. If the answer to this first question is that there are no establishments in the Union, then DSOs and researchers should each consider if the targeting criterion (Article 3(2) GDPR) applies to them (see below at paras 150 – 153).

146. **Secondly**, if the answer to that first question is yes, then DSOs and researchers should each consider if any research processing activities are carried out *"in the context of the activities of"* that establishment in the Union:

    a) If a DSO or researcher has an establishment in the Union and that establishment in the Union is conducting, coordinating or otherwise has responsibility for the relevant processing (even if the actual data processing is taking place outside the Union), the research processing will be conducted in the context of that establishment in the Union. The location of the data subjects is not important to this analysis because the application of the GDPR is not limited to individuals in the Union.

    b) The situation is more complex if a DSO or researcher is based outside the Union and the research processing occurs outside the Union. In this case, the DSO and/or researcher will each need to analyse the links existing between the processing that is conducted overseas and the establishment(s) it has identified in the Union. Even if the local establishment in the Union is not playing any role in the research, the research processing by the overseas researchers may still be "inextricably linked" to the activities of a local establishment, for instance if the local establishment is funding the research.

    c) Where multiple entities, some inside and some outside the Union, are jointly determining the purposes and essential means of processing, the existence in the group of one or more establishments in the Union could bring the others within the scope of the GDPR where the research processing takes place in the "context of the activities of an establishment" in the Union. This is a complex question, and the analysis will be fact specific. Data controllers in such situations should seek specific advice on whether they are within the GDPR's scope.

147. If both these questions are answered in the affirmative, their research processing is subject to the GDPR based on Article 3(1). In turn, DSOs and researchers will

each need to consider where in the Union the relevant establishments are located for those research activities. These locations will have an impact on which Member State laws they must comply with, and which supervisory authority will be responsible for dealing with that activity. Further considerations arise in this context:

a) DSOs and researchers will each need to ensure they are aware of and comply with the additional conditions and frameworks in the Member States in which they are established, such as provisions concerning Article 9 (processing of special categories of personal data) and Article 23 (restrictions).

b) If a controller has a single establishment, the local supervisory authority in the establishment Member State will generally be its lead supervisory authority for complaints about the processing (even where research processing impacts data subjects in multiple Member States). The exception is where a complaint relates *only* to an establishment or data subjects located in a different Member State.

c) If a controller has multiple EU establishments, it should determine where its "main establishment" is for the research processing as this will indicate its likely lead supervisory authority (though the controller's analysis is not legally determinative). This requires a factual analysis of the establishment where the decisions on the purposes and means of the research activity are taken. DSOs and researchers cannot "forum shop" for favourable jurisdictions.

d) If the research activities take place in the context of multiple establishments (including where there are joint controllers), then a DSO or researcher must ensure they are aware of and their processing complies with the conditions and frameworks in all the Member States in which the establishments are located.

148. DSOs and researchers should be aware that individuals may lodge complaints with a supervisory authority and/or bring court proceedings either where the DSO or researcher is established or where the data subject has their habitual residence. If a data subject makes a complaint in the context of cross-border processing (e.g. where the processing impacts data subjects across multiple jurisdictions or the DSO or researchers have multiple establishments), the lead supervisory authority will have primary responsibility for dealing with the complaint together with any other concerned supervisory authorities.

149. Individuals' rights over their data may depend on the Member State in which they "habitually reside". These must be honoured by DSOs and researchers when responding to a rights request (see Section 5) where that individual can be identified.

Targeting criterion and associated considerations

150. If a DSO or researcher is processing data for research purposes and that processing is not related to an establishment in the Union, it must still consider whether the "targeting criterion" applies to its processing to determine if the GDPR applies. Joint controllers can conduct this analysis jointly.

151. The targeting criterion applies if the DSO or researcher processes personal data, and that processing is related to (i) offering goods or services to those individual data subjects in the Union or (ii) monitoring those individuals' behaviour in the Union. Of the two, the latter is most likely to apply but that will depend heavily on the nature of the research undertaken. In order to understand whether the monitoring condition is met, the parties should consider factors such as (i) whether the research involves 'real-time' and continuous surveillance of data subjects, against purely considering a set and historic dataset (ii) whether research follows defined cohorts of individuals through time, and (iii) whether any decisions affecting the individuals result from the processing.

152. The targeting criterion is only met where the monitoring both (i) concerns behaviour in the Union and (ii) is of data subjects in the Union. That is, the data subjects must be in the Union when the monitoring takes place. Thus, a non-Union established researcher monitoring data subjects located outside the Union will not meet the criteria, even if some of the past behaviour being monitored took place in the Union.

153. If DSOs or researchers are subject to GDPR on the basis of the targeting criterion, they will each need to appoint a representative in the Union if they do not already have one for their core purposes. They can do this jointly if they are joint controllers. The appointment of a representative does not constitute an "establishment" for Article 3(1) purposes. If a data subject makes a complaint or brings court proceedings these will occur via the representative.

Transfers of data to third countries

154. Chapter V GDPR contains transfer rules that apply when an entity that is subject to the GDPR transfers personal data to a separate entity in a third country. In order to be lawful, such transfer must be covered by (i) an adequacy decision, or (ii) appropriate safeguards for data subjects' rights.

155. The meaning of transfer is extremely broad: it does not require a physical handover of data and can include remote access from a third country. In practice, whenever data is being shared between DSOs and researchers, there will be a transfer if the receiving party (whether DSO or researcher) is based in a third country. Sharing data with other individuals within the same organisation will not constitute a transfer, even if those other individuals are located in a third country. A transfer will however arise where data is shared from one joint controller to another, the latter being based outside the EU. Where data is shared between different research organisations, as might occur within a research consortium, a transfer could arise because data is being shared between legally separate entities.

Adequacy decisions

156. Adequacy decisions record a determination based on Article 45 GDPR that a country (or a territory or sector thereof), or international organisation outside the EU offers an adequate level of data protection. DSOs and researchers, once they have identified any international data transfers involved in the research project, should consult an up-to-date list of adequacy decisions prior to any transfer, to check if it is lawful on this basis.

Appropriate safeguards

157. If no adequacy decision can be relied upon, appropriate safeguards pursuant to Article 46 GDPR are required to ensure the transfer is lawful. The most relevant appropriate safeguards in the DSO to researcher data sharing context are (i) data protection contract clauses (such as the model Data Sharing Agreement), and (ii) a Code of Conduct approved under Article 40 GDPR. To the extent this Code is approved, and DSOs and researchers undertake to comply with it through binding and enforceable commitments, it could be used as an appropriate safeguard for transfers in the absence of an adequacy decision.

Derogations

158. There are some further derogations from transfer rules provided for by Article 49 GDPR. The main derogation that may be of relevance in the DSO to researcher context is where the transfer is necessary for "important reasons of public interest". The requirement for "important reasons" is a higher standard than provided for in the exemptions and derogations requiring processing to be in the public interest. Such derogations cannot be used as a permanent, recurring basis for transfer of data.

159. Transfers relying on such derogations can only take place if the transfer is "not repetitive", concerns "only a limited number of data subjects", is to be balanced against the "interests or rights and freedoms of the data subject" and requires the controller to demonstrate that they have "assessed all the circumstances

surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data." The controller must also inform each data subject of the transfer and the interest pursued. Member states can also "expressly set limits" to the "transfer of specific categories of personal data to a third country or an international organisation".

160. For these reasons, this derogation will only be relevant to DSO to researcher data sharing in very limited circumstances but should be considered if all other options for making an international transfer lawful have been exhausted.

Considerations for DSOs and researchers

161. DSOs and researchers should each assess whether the GDPR will apply to each of the processing activities involved in their research on the basis of either (i) the establishment criterion or (ii) the targeting criterion in advance of sharing data for research purposes.

162. If a DSO is established in the EU for its core purposes, the further sharing of that data for research purposes will also be within the scope of 3(1) GDPR. If a DSO is not established in the EU for its core purposes, and it shares data with a researcher, that will not by itself trigger establishment[12]. However, it will need to consider if that further processing for the purposes of the research falls within Article 3(2) GDPR. If a DSO's processing for its core purposes falls within scope of Article 3(2), a new assessment should always be made of whether the sharing of that data for research purposes falls within Article 3(2).

163. DSOs and researchers should be open and transparent with each other about whether the GDPR applies to their research processing activities. DSOs and researchers should each ensure they are aware of relevant Member State laws in the jurisdictions in which they are established and of their lead supervisory

[12] If the DSO and researcher are joint controllers, specific advice should be sought.

authority and be open and transparent with each other about this. Insofar as it is reasonably practicable, and without unduly delaying or constraining research, these jurisdictional matters should be documented by DSOs and researchers through their data sharing agreement.

164. Each party should be able to rely on the position taken by the other regarding the laws that apply to it. However, if the parties are unable to agree on the applicability of GDPR or questions of jurisdiction, they may consider submitting a summary of the data processing they propose to an independent expert body for assistance.

165. If only one of the parties is subject to the GDPR for the research processing, the other party should be mindful of the other's need to comply with the GDPR and ensure that data is shared in a manner that facilitates that compliance. Similarly, where parties are based in different Member States, they should be mindful of each other's need to comply with the additional conditions and frameworks in the Member States in which they are established and ensure data is shared in a manner that facilitates that compliance.

166. DSOs and researchers should work together to map all transfers in advance of data sharing, including any onward transfers and transfers to processors and should be open and transparent with each other about these transfers. These transfers should be documented by DSOs and researchers through their data sharing agreement. DSOs and researchers should also notify each other of the existence of any international transfers that were not previously agreed on in advance of making those transfers.

Part II: Implementation & Safeguards

1 Introduction

This Code provides for a range of approaches to structuring a research project and the data sharing underpinning it. It is anticipated, however, that the most common use of the Code will be to support data sharing from a platform to a researcher where the platform does not determine the purposes and means of the processing by the researcher. That is, the platform, acting as a data-sharing organisation (DSO) will not be a joint controller of the research processing.

Practical implementation of the Code in this scenario will move through the following broad phases:

DSO has made / makes available **Codebooks (Section 2)**, which indicate to researchers what data may be available for qualifying research

Researcher formulates **research proposal (Section 3)**, comprising a **Data Needs and Management Plan (Section 4)—which itself includes an assessment of the risk level of the research (Section 5)** and selection of **safeguards (Section 6)**—and **methodological and ethical review (Section 7)**

Annex 1 provides a checklist for researchers to confirm when they are ready to submit a request for data sharing to a DSO

DSO **reviews proposal (Section 8)** to ensure that it is for qualifying research and that the proposed safeguards are appropriate

Annex 2 provides a checklist for DSOs to confirm they have sufficient information to enter into a data sharing agreement and share data

DSO and researcher enter into a data sharing agreement that incorporates the details of the research proposal and binds them to implementing the agreed safeguards

This Part II guides DSOs and researchers in implementing these phases in practice. It focuses on a typical project in which DSOs and researchers are not joint controllers for the research processing. This Part II retains relevance for such joint controller scenarios, but in such cases DSOs and researchers should consider carefully how to apply the guidance to their specific situation[13].

2 Codebooks

DSOs must make Codebooks available to researchers – publicly and through established channels of communication with the research community – in relation to data or datasets that may be available for research pursuant to this Code. They must establish and maintain processes through which researchers can submit questions about Codebooks and about the potential availability of data not included in any Codebooks.

2.1 Contents of Codebooks

A Codebook will include, at minimum:

a. A description of the categories of data contained within the dataset (the "Data Fields"), including the presence of any data that engages Articles 9 or 10 GDPR;

b. A description of the categories and approximate number of data subjects represented within the dataset;

c. A description of what the dataset represents and its fitness for research, including: (i) the completeness of the dataset (e.g., relative to the available data held by the DSO or another definition of the relevant population), (ii) the correctness of the dataset (e.g., the degree to which the data within it

[13] In particular, joint controller scenarios will require greater coordination between platforms and researchers when assessing data processing risks (Section 5) and safeguards (Section 6) and, in some instances, in preparation and review of the research proposal (Section 8) and methodological and ethical review (Section 7).

is known to be true – both specificity and precision); and (iii) the timeliness of the dataset (e.g., the degree to which the data represent reality from a particular point in time);

d. A list of the country(ies) in which data subjects represented within the dataset are located, if known;

e. A description of any relevant privacy or other settings that apply to the data, including, without limitation, settings selected by data subjects to limit the disclosure of the data to specific audiences; commitments by the DSO not to disclose or use data in certain ways; or requests by data subjects to restrict or otherwise limit the use or disclosure of data;

f. A high-level description of any measures taken by the DSO to pseudonymise the data ("Pseudonymisation Methods"), and of any error, bias, or variance that Pseudonymisation Methods may introduce into the dataset;

g. An initial, high-level assessment of the risk level that the dataset or specific Data Fields might indicate, by reference to Section 5[14]; and

h. Any other information reasonably likely to be necessary for a researcher to discharge its obligations under this Code.

A Codebook must provide sufficient level of detail and explanation to enable researchers to discharge their obligations under the Code, without containing any personal data of any of the data subjects within the dataset.

[14] Platforms will only be able to give a very high-level indication of risk level, as risks to rights and freedoms of data subjects arise from the *processing* that researchers will carry out, which platforms will not generally be aware of in advance in this scenario.

Researchers may request additional information concerning a dataset from a DSO as reasonably required to enable them to evaluate their own obligations under the Code in connection with a proposed research project.

2.2 Pseudonymisation Methods

DSOs may apply one or more Pseudonymisation Methods to datasets before making them available to researchers. At the time of doing so, DSOs should document, for inclusion in the Codebook (or separate communication to researchers if necessary as a security measure):

a. The specific Pseudonymisation Methods used;

b. Whether any Data Fields have been altered or aggregated, and the effect of any such alteration or aggregation;

c. A description of any potential error, bias or variance the Pseudonymisation Methods may have introduced into the dataset; and

d. To the extent known, a quantification of the level of error, bias or variance introduced.

2.3 Dataset Optionality

DSOs should prepare datasets with different options that can be selected by a researcher depending on the needs of the research and document these options in the Codebook. This may include:

a. The option to remove Data Fields that are not relevant to a specific project; or

b. The option to select different levels of aggregation of a Data Field, for example, “age range” vs. “birth year”.

3 Preparing a research proposal

To make use of the Code, researchers must prepare a research proposal augmented with specific elements that enable both the researcher(s) and DSO(s) to ensure compliance with their obligations under the GDPR and the Code. The research proposal must include:

a. A **Data Needs and Management Plan** (Section 4), including a **Risk Assessment** (Section 5) and description of **Proposed Safeguards** (Section 6);

b. Confirmation of **ethical review** (Section 7); and

c. Confirmation of **methodological review** (Section 7).

4 Data Needs and Management Plan

The Data Needs and Management Plan is used to set out the *specific purpose* for which data – including data engaging Articles 9 and 10 GDPR – are requested from the DSO, tying this justification to the research questions, hypotheses, and/or objectives of the research project.[15] The Data Needs and Management Plan must be approved by the researcher's institutional data protection officer (DPO) in writing, with a copy of the approval retained for inspection by the DSO. It must be updated and reviewed by an institutional DPO at a minimum every 12 months.

Researchers may not know the precise data needs of a research project at the outset of the project, especially when the research is exploratory. To address this, researchers relying on this Code must:

- Begin their research with the minimal data needed at the outset.

[15] Note that there is considerable overlap between the information required in the Data Needs and Management Plan (DNMP) and Legitimate Interests Assessment (LIA). Researchers and their institutions should ensure these documents are harmonised.

- In the Data Needs and Management Plan identify additional data that may be needed, flagging that need for DPOs and the DSO(s) as a potential follow-up request.

- In circumstances where that additional data would be lost should it not be collected or accessed at the outset of a research project, researchers must

    - Highlight this in the Data Needs and Management Plan;

    - Avoid processing this data and apply appropriate additional safeguards (e.g. indicating that these are additional data that may be needed in the metadata); and

    - Destroy this data as soon as it is confirmed to be unnecessary.

- Re-evaluate data needs at regular intervals, updating the Data Needs and Management Plan as necessary.

In some circumstances, the mechanism of data access (e.g. a real-time Application Programming Interface) may make more data available to researchers than is needed for the research purpose. In such cases, it is the responsibility of the researchers to expediently delete all unnecessary data. Plans for doing so should be detailed in the Data Needs and Management Plan.

The Data Needs and Management Plan ("DNMP") comprises:

4.1 Research overview

Research Team: (i) the identity, contact details, and CV of the principal investigator and each known additional individual researcher (or required qualifications where recruitment is ongoing) that will access the dataset; (ii) a description of the research institution; and (iii) the identity and contact details of an authorized representative of the research institution.

Research Description: a description of the research that includes an overview and explanation of (i) the research objectives, (ii) the research questions, (iii) the hypotheses to be tested, or, in the case of exploratory research, the justification for conducting the exploratory research.

For exploratory research, the DNMP's Research Description must include:

- An overview and explanation of the research purpose, including research objectives.
- An overview and explanation of known research questions.
- A justification for approaching this as *exploratory* research (i.e., What is unknown that requires further exploration before a more systematic analysis can be conducted?).

It is particularly important that the exploratory nature of the research be well-justified to ensure that such work does not serve as a basis for side-stepping data minimization requirements under the GDPR.

For research involving full, systematic analysis, the DNMP's Research Description must include:

- An overview and explanation of the research purpose, including research objectives.
- An overview and explanation of the research question(s).
- Where applicable, an overview and explanation of the hypotheses to be tested.

4.2 Data needs

Information about the data requested, namely:

- The Data Fields and required granularity requested

- For personal data, a justification of the data's necessity to the research purpose described in the Research Description. The DNMP must explicitly identify the research objectives, questions, and/or hypotheses for which the personal data are needed[16].
- Additional data to be added to and/or combined with the platform data (if any).
- The intermediate and final Output Data the research is expected to generate. (See Section 5.3)

4.3 Risk assessment

The information detailed in Sections 4.1 and 4.2 should form the basis of a risk assessment answering the questions outlined in Section 5 of this Part II and identifying the quadrant in which the research project falls, per *Figure 1*.

4.4 Proposed safeguards

Based on the risk assessment, the DNMP must detail the safeguards the researcher(s) propose to implement in handling the requested data. This includes plans and protocols for data storage (including specified retention periods and criteria), destruction (e.g., when unneeded or at the end of the data storage period), security, and access. This section of the DNMP should explain how the recommended safeguards in Section 6 will be applied to the project.

5 Risk assessment framework

The right combination of safeguards will depend on the risks involved in each research project. Safeguards must be appropriate to the nature and purpose of the processing and the risks posed to the rights and freedoms of individuals. Such risks cannot be predetermined but must be assessed in relation to each processing activity.

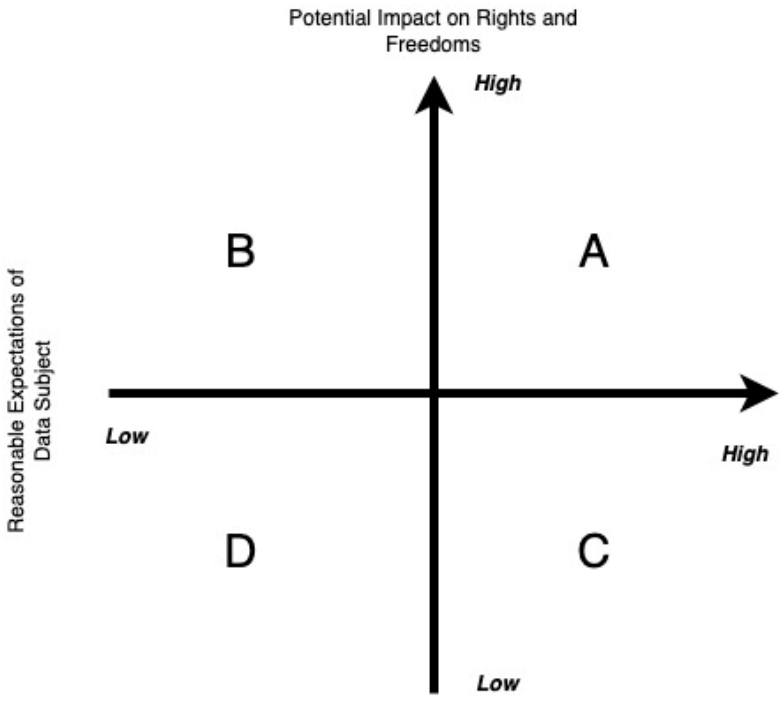
[16] This information and reasoning can be used in the context of the legitimate interests assessment (where that legal basis is relied upon for the research) in order to avoid duplication of effort.

When assessing the level of risk potentially posed by data processing activities, researchers and DSOs must consider:

- The **reasonable expectations of data subjects** in relation to the processing. This includes a consideration of how private the data subjects might reasonably expect the data to remain, given the circumstances of the data's generation.
- The **potential impact on data subjects' rights and freedoms** of the processing. This involves a consideration of how the proposed processing does impact rights and freedoms, as well as how it could do so, including if the data or its research outputs were misused.

In the following framework, these attributes are mapped along a continuum of low-to-high risk, and the two dimensions then combined to form a risk framework with four quadrants, as pictured in Figure 1.

Figure 1: Reasonable Expectations and Potential Impact Risk Framework



Potential impact relates to a broader category of risk than reasonable expectations, and so this framework gives greater weight to potential impact risks. The four quadrants in Figure 1 are therefore labelled A, B, C, and D, moving from greatest to lowest combined risk.

Processing in Category A will require the greatest safeguards, processing in Category D the least. However, even Category D processing will require safeguards (see Section 6.1).

5.1 Reasonable expectations of data subjects

Users of the Code must consider what is reasonable for a data subject to expect in relation to both (i) the data to be processed and (ii) the way in which it is to be processed. Research processing that is not within reasonable expectations will still be permitted (subject to compliance with Part I and the GDPR), but creates a higher degree of risk, necessitating higher levels of safeguarding. Processing that is well within reasonable expectations will be lower risk but will still require some safeguards.

This assessment must include, in particular, the context in which the data to be processed was generated, and therefore the level of privacy and protection of information that data subjects are entitled to expect in relation to it. The lower the expectation of privacy, the lower the risk level. In general, data subjects are less entitled to expect privacy in relation to data they have put in the public domain, such as publicly available social media posts. It will be relevant to consider (independently of the proposed research processing):

- The likelihood that the data has reached or will reach a substantial public audience. (The posts of a notable public figure, for example, might be considered more in the public domain than those of an ordinary user.)
- What a reasonable data subject would understand regarding the extent to which their data is publicly available, taking into account platform features and conventions. (See Case Studies 1 and 2 below).

The assessment must distinguish between raw data (e.g., copies of posts, profile information, engagement data) that may be in the public domain and any inferences drawn from that data through research, which by definition will not be public.

Platform Case Study #1 – Twitter[17]

Twitter is a relatively public medium, but not all content is equally public. Consider the following:

- The vast majority of Twitter content is posted publicly.
- Public content appears in a user's profile and in other users' newsfeeds, and other users do not need to follow the original poster (OP) for OP's content to show up in their feeds.
- Anyone whom the OP has not blocked, including those not signed up to the service, can view public content.
- Any un-blocked Twitter user can interact with public content.
- One user may follow another without the latter's approval or reciprocation.
- Tweets are frequently picked up and further publicized off-platform by journalists and others.

Given these platform features, Twitter users are more likely to understand that the information they share is available to a large public audience. However, these features and conventions do not mean that everyone understands this equally[18], and considerations of relative expectations should take who the data subjects are into account. Reasonably, politicians, public officials, media personalities, celebrities, digital influencers, etc.—and especially those with substantial follower counts—will understand and expect that the content of their tweets is public.

[17] This case study was formulated in and based on Twitter's features as of May 2022.

[18] A survey conducted by the Pew Research Center in May 2021 found that a substantial number of US Twitter users with public accounts believed that their accounts were private. (See https://www.pewresearch.org/internet/2021/11/15/the-behaviors-and-attitudes-of-u-s-adults-on-twitter/.) See also the UK Centre for Data Ethics and Innovation's March 2002 report on the public understanding of AI (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1064525/Public_attitudes_to_data_and_AI_-_Tracker_survey.pdf.)

Platform Case Study #2 – Facebook[19]

Facebook presents a more complex case, with multiple features and spaces within the platform that present varying levels of publicness.

To start, consider the way content is shared on users' profile pages:

- Facebook users may post publicly to their profile pages, with content then viewable to anyone on- or off-platform.
- However, it is also possible - and relatively common - for users to limit their audience. For example, users may choose to share a post to just their friends on Facebook. They may even further limit visibility to specific friends.
- Users' profile posts—even their public posts—are much less likely to be picked up and further publicized off-platform by journalists or others, compared to Twitter.

Given these features and conventions, Facebook users posting publicly to their profile pages are even less likely than Twitter users to understand and expect that their information could reach a large public audience. Thus, the fact that these posts are public does not, on its own, limit data subjects' reasonable expectations of privacy.

However, Facebook also includes public Groups and Pages, where, in many cases, the reasonable expectation of privacy is likely to be lower.

Meta describes Facebook Groups as "a place to communicate about shared interests with certain people," further noting that "you can create a group for anything – your family reunion, your after-work sports team or your book club"[20]. Meta also suggests that Groups offer a way for businesses, including influencers, to "build up a fanbase" and connect people to their brand and content[21]. The purpose of a public Group is then highly relevant to considerations of a data subjects' expectations. On the one hand, posts in a Group for a family reunion are not highly public, since the intent, even if the Group is set to "public," is to communicate with a small, defined group of people, not to reach a wider audience. On the other hand, posts generated by a media personality in a public Group that was created to expand and communicate with their fanbase are highly public. Even within such a Group, however, posts and comments by average users are relatively less public.

Finally, consider Facebook public Pages. Meta describes Pages as intended "for businesses, brands, organizations and public figures to share their stories and

[19] This case study was formulated in and based on Facebook's features as of May 2022.

[20] See https://www.facebook.com/help/1629740080681586.

[21] See https://www.facebook.com/business/learn/lessons/use-groups-build-community.

connect with people"[22]. And when creating a Page, one must select from a list of categories that reflect the "type of business, organization or topic the Page represents"[23]. The intent of Pages is therefore very clear, and Page creators are particularly likely to understand that their posts are public and to intend for them to reach a wide audience. Thus for public pages, a data subject would have a lower reasonable expectation of privacy.

5.2 Potential impact on rights and freedoms

Assessment of the risk from potential impact on rights and freedoms must consider how the proposed data processing and its outputs could be either used or misused in ways that impact data subjects. As a starting point, users of the Code must consider the special category traits listed in Article 9 GDPR, but the consideration of impact must be a broad one.

The assessment must include not only the nature of DSOs' and researchers' own data processing, but also the impact of unauthorised access (or other processing) of the data concerned. One should therefore ask questions such as:

- Could sensitive information about individuals (including the traits listed in Article 9 GDPR) be gleaned from the processing in isolation?
- Are other data present where datasets or results are being stored, or that could be brought into that storage location, that, combined with the dataset in question, could reveal such sensitive information?
- What is the probability that someone could inadvertently reveal sensitive information about data subjects or otherwise infringe their rights and freedoms?

[22] See https://www.facebook.com/help/104002523024878.

[23] See https://www.facebook.com/pages/creation/?ref_type=facebook_business_website.

- What is the probability that someone could intentionally (i) access research data or results, and (ii) reveal sensitive information about data subjects or otherwise infringe their rights and freedoms?

5.3 Research Outputs

To properly assess risk levels, researchers must consider both the data serving as *inputs* into a research project and *the data that result from* - i.e., are outputs of - the research itself ("Output Data"). Such Output Data might be generated in intermediate phases of research or be the final results of the research.

By way of illustration, consider the following scenario:

Scenario 1: Sensitive inferences from innocuous data

Researchers at University X seek access to a social media dataset comprising public posts about celebrities and entertainment topics. The raw input data indicates a relatively low level of risk, as it consists of public posts and seemingly innocuous topics. However, the researchers are interested in exploring when and how users politicize entertainment content, and they hypothesize that this will vary by users' political ideology. The researchers do not have individual-level data (e.g., survey data) about their users' political ideology, but they plan to apply a computational model that allows them to infer users' political ideology on the basis of the accounts the users follow. Thus, though the original data appears relatively low-risk, the processing is likely to fall outside data subjects' expectations and, if not protected, could have adverse impacts on their rights and freedoms. The researchers should therefore make plans to protect the inferential data (a form of Output Data) by implementing safeguards appropriate for Category A.

5.4 Ongoing assessments

Although an assessment must be prepared at the outset of a project in order to make a request for data, risk assessments are not static and must be performed as new data are added to or generated by the research. Researchers may not know that their processing will fall into a higher risk category until the research is underway, but once this is known, it should be accounted for in the technical and/or organizational safeguards. As noted in Section 4 of Part I, DSOs and researchers should therefore include regular risk (re-)assessments as part of their data management plans.

5.5 Who assesses risk?

This Part II assumes that researchers are the data controllers for the research processing they will carry out, and DSOs are not joint controllers. Thus the researcher will carry out the risk assessment and selection of safeguards for their processing, which will be both certified by their institution and reviewed by the DSO. (See Section 8). The DSO will assess the risks involved in preparing and providing access to the datasets.

Joint controllers must jointly assess the risks involved in their processing, working together in good faith to (a) realistically evaluate processing risks and (b) strike the appropriate balance between the rights of data subjects and the need for and value of scientific and historical research. If agreement cannot be reached, the parties may consider referring their proposed risk management arrangements to an independent third party with expertise in the processing of personal data for research.

6 Required and Recommended Safeguards

Technical safeguards comprise measures involving technology and the policies and procedures in place for the use and implementation of that technology. Technical safeguards may be implemented, for example, to address access control, data security, and monitoring and compliance needs. Organisational safeguards comprise all non-technical measures, including policies and procedures for laying out and reviewing research plans, evaluating the legal and ethical implications of the research, and assessing the capacity of the researcher(s) to implement the research and its safeguards, among other considerations.

Drawing on best practices from a variety of scientific, public sector, and industry research and data access regimes, the proposal for a Code of Conduct requires DSOs, researchers, and researchers' institutions to implement certain technical and organisational safeguards for each category of risk.

These requirements and recommendations are generally cumulative, with safeguards in lower categories of risk in many instances also required in higher risk

categories. The following section therefore outlines safeguards required and recommended for all risk categories, including the lowest risk, Category D. The section then discusses safeguards required and recommendations for medium risk, Categories C and B, and ends with safeguards required and recommended for the highest risk processing, falling in Category A.

6.1 Safeguards for all risk categories, including low-risk processing (Category D)

Part I outlines DSOs and researchers' duties to meet their GDPR transparency obligations, which may include transparency safeguards (such as making information public) where relying on an exemption. It also requires DSOs and researchers to put in place measures to communicate about and give effect to the exercise of data subject rights. This section outlines safeguards focused on data practices of the research processing.

6.1.1 Data minimisation (required of researchers)

The GDPR requires that processing activities only involve personal data when it is *necessary* to achieve the purpose at hand. Researchers must therefore consider at the outset whether the objectives of the research could be achieved without processing personal data, or with less personal data.

In practice, this means carefully considering the types of data requested (e.g., individual-level vs. aggregate data, text data vs. engagement data) and what Data Fields (variables) are necessary to the research, clearly documenting this reasoning in the DNMP.

6.1.2 Ethical and methodological review (required of researchers)

Processing will be for qualifying research under this Code where it meets ethical and methodological standards for academic research (see Preamble). All researchers relying on this Code must therefore have their intended research reviewed and approved by qualified persons. (See Section 7.)

Ethical and methodological review also serves as a mechanism for safeguarding the rights and freedoms of data subjects by ensuring a link between the data requested

and the research objectives, and justifying any risk to data subjects' rights and freedoms by reference to the benefits of the research.

6.1.3 Pseudonymisation (recommended, where appropriate, for DSOs and researchers)

Pseudonymisation of data is specifically mentioned by the GDPR as a technique that may serve as an appropriate safeguard. It will be appropriate in many research contexts, whether the processing falls into category A, B, C or D. The appropriateness of this technique should, however, be considered in relation to (i) the impact it would have on the proposed research, and (ii) the other safeguards that are (or can be put) in place to protect data subjects' rights. Where pseudonymisation would significantly impair the research objectives, other safeguards (especially those indicated for medium and higher risk processing) may provide the appropriate protection for data subjects' rights, allowing the research to be carried out using data that is directly referable to identified individuals.

Where pseudonymisation *is* used, DSOs and researchers should match its robustness to the risk category of the research processing. In particular, for higher-risk processing, in-depth consideration should be given to the risk of reidentification (i.e., reversal of the pseudonymisation). DSOs and researchers should consider not just their own proposed processing, but also the risk involved should other actors obtain the data:

- What is the probability that someone could accidentally re-identify data subjects by conducting analysis on the dataset in question?
- What is the probability that someone seeking to re-identify data subjects could (i) access the data and (ii) re-identify data subjects from it?
- Is there other data present where the dataset is being stored, or that could be brought into that storage location, that would contribute to re-identification attacks?

These questions prompt data controllers to think carefully about how data could be used beyond their own purposes. Even if researchers have no intention of re-identifying pseudonymized data, steps should be taken to minimize the chance that another actor could re-identify individuals by combining research data or outputs with other available data. Consider, for example, Scenario 2:

Scenario 2: Aggregated results with sparse observations

Researchers at University Y have received access to a social media dataset comprising aggregated (i.e., robustly pseudonymised) data for posts about self-harm. Their findings reveal that just a handful of users interact with self-harm posts at very high rates. This finding itself makes it easier to re-identify those users individually, even without employing sophisticated statistical techniques. This reduces the safeguarding impact of the pseudonymisation and suggests that other safeguards may need to be implemented for these Output Data.

6.1.4 Training on safe and ethical data use (recommended for researchers)

Researchers relying on the Code are strongly recommended to complete training on safe and ethical uses of data. For example, the Consortium of European Social Science Data Archives offers a "Data Management Expert Guide" training course that covers a number of relevant ethical and data management topics.

Because such training programs are only beginning to be developed across Europe, the Code does not yet list this a requirement. However, in the future, such training may become a prerequisite for receiving approval for a Data Needs and Data Management Plan. A graduated training system might also be developed—under which higher levels of training would facilitate greater access to riskier forms of data.

6.1.5 Data pipeline auditing (recommended for DSOs)

In order to ensure that the results and insights drawn from scientific and historical research covered under this Code are accurate, DSOs should provide mechanisms

for audits that verify the accuracy and completeness of the provided data. At minimum, such audits should include:

- Data pipeline code review checks performed by qualified researchers who do or will make use of the data. Where appropriate, such code should be made public.
- Use of real or synthetic data, supplied by researchers, to test the output of data pipelines.

For static datasets, a data pipeline audit could be performed as one of the final steps before dataset release. For dynamic data, data pipeline audits should be performed at regular intervals, no less than six (6) months apart.

DSOs should report the results of those audits to all researchers who have or have had access to the relevant data.

6.1.6 User registration (recommended, where applicable, for DSOs)

In many instances, researchers will rely on DSO systems to access data—for example, when collecting data via APIs. In such cases, DSOs should implement a user-friendly registration system that gathers minimally-intrusive information necessary to verify a researcher's identity, credentials, and institutional affiliation, as well as basic contact information. DSOs may also use this process to verify that researchers have received the various approvals required within the Code—for example, by requesting that researchers upload approval letters.

Table 2: Safeguards for all risk categories, including low-risk (Category D) processing[24]

Safeguard	Required or Recommended	Individual Researcher Role	Research Institution Role	DSO Role
Data minimisation	Required	Plans (via DNMP) and implements	Reviews and approves	Reviews DNMP
Ethical and methodological review	Required	Plans and implements	Reviews and approves	Has sight of confirmation
Pseudonymisation	Recommended, where appropriate	Plans and implements	NA	Plans and implements
Training on safe and ethical data use	Recommended	Undertakes	May provide training	NA
Data pipeline auditing	Recommended	Selected qualified researcher(s) perform(s)	NA	Plans and supports implementation
User registration	Recommended, where applicable	Provides requested information	NA	Implements

6.2 Safeguards for medium-risk processing (Categories C and B)

All requirements and recommendations described in Section 6.1 apply to medium risk processing. However, as risk increases, additional safeguards are necessary. This section also discusses the recommended means of data access for medium-risk processing—i.e., access-restricted APIs. The Code recommends, rather than requires, this mechanism, because in some circumstances (discussed in Section 6.2.1), a more restrictive access mechanism (i.e., use of a data clean room) may prove preferable to researchers.

[24] Note that in order to provide clarity, this table and tables 3 and 4 delineate the roles of the individual researcher (who will not normally be a data controller, see Part I), and the research institution. Users of the Code should interpret the table in the context of their specific combination of data controllers.

6.2.1 Means of data access – Access-restricted API (recommended for DSOs)

Access-restricted application programming interfaces (APIs) are particularly well-suited to medium-risk, Categories C and B, data. DSOs should establish and manage access to these APIs, enabling approved researchers to export and store the retrieved data within the researchers' own secure systems.

In approving access, DSOs should establish a user registration mechanism (see Section 6.1.6) that includes a means of verifying that researchers have received the approvals summarized in Table 1.

When providing access in the context of medium-risk processing, APIs should generally include:

- An access authentication mechanism (e.g., via two-factor authentication or secure VPN)
- Penetration-tested security features to prevent unauthorized access and to prevent authorized users from exporting data for which they are not approved, with regular evaluation to assess whether the features remain state-of-the-art
- Monitoring and auditability of researcher actions (e.g., researcher data queries), with regular reports provided to the researcher of their actions

In certain circumstances, researchers may prefer to access medium-risk DSO data in a virtual clean room (see Section 6.3.1) that prevents data export. For example, if researchers are concerned that, should they host their own data, it would be subject to state or other surveillance, maintaining data within a DSO's systems may prove advantageous. This may also be true for researchers at institutions lacking capacity to implement appropriate technical safeguards for hosting data in medium-risk contexts. (See Sections 6.2.3 and 6.2.4.) The Code therefore recommends, but does not require, that access-restricted APIs serve as the means of access in medium-risk contexts. However, when it is not advantageous for a researcher to use a virtual clean room, data access in medium-risk contexts should be provided via an API.

6.2.2 Data encryption (required, where applicable, of researchers)

In medium-risk circumstances where researchers are storing data on their own (or their institution's) systems, encryption at rest must be applied in Category B and is recommended for Category C. Encryption in-transit is required for approved transfer (e.g., between approved researchers at different institutions) of all medium-risk processing (Categories C and B).

6.2.3 Access restrictions (required, where applicable, of researchers)

In medium-risk circumstances where researchers store data on their own, or their institution's, systems, safeguards must be in place to limit access to authorized users. At minimum, password-protection must be applied in Category C, with password protection and either two-factor authentication or secure VPN access required in Category B.

Access to relatively sensitive data points must be restricted to only those members of the research team who require access. This may necessitate storing more sensitive data separately from less sensitive data and/or generating and separately storing different versions of the datasets.

When devising access restrictions, researchers and their institutions should consider the likelihood that future researchers will require access for scientific replication purposes and must, where needed, establish secure mechanisms for such access in line with this Code.

6.2.4 Data destruction (required, where applicable, of researchers)

In general, under this Code, researchers must swiftly—within no more than 90 days—destroy:

- Any personal data that was collected or generated inadvertently.
- Any personal data that is not necessary to the research purpose (see Section 6.1.1).

At the end of the research project, DSOs and researchers should comply with the GDPR's principles on storage limitation and the plans for data retention set out in the DNMP.

Table 3: Safeguards for medium-risk processing (Categories C and B)

Safeguard	Required or Recommended	Researcher Role	Research Institution Role	DSO Role
Access-restricted API	Recommended	Provides required information; accesses under provided conditions	NA	Establishes and oversees
Data encryption	Required, where applicable	Plans and Implements	Reviews, approves, and assists with implementation, where applicable	NA
Access restrictions	Required, where applicable	Plans and Implements	Reviews, approves, and assists with implementation, where applicable	NA
Data destruction	Required, where applicable	Plans and Implements	Reviews, approves, and assists with implementation, where applicable	NA

6.3 Safeguards for high-risk processing (Category A)

6.3.1 Means of data access – Virtual clean rooms (required of DSOs)

For high-risk processing (Category A), DSOs must provide access within a secure virtual clean room. These digital environments must permit researchers to import their own data, perform research analyses, and export the results of their analyses.

However, such clean rooms must implement technical safeguards to prevent the export of high-risk DSO data.

When providing access to data in the context of high-risk processing, virtual clean rooms must include:

- An access authentication mechanism (e.g., via two-factor authentication or secure VPN)
- Penetration-tested security features to prevent unauthorized access and to prevent authorized users from exporting data for which they are not approved, with regular evaluation to assess whether the features remain state-of-the-art
- Monitoring and auditability of researcher actions (e.g., researcher data queries), with regular reports provided to the researcher of their actions

DSOs must enable access to virtual clean rooms for peer review and study replication purposes and retain data, where not in conflict with data subject's requests, to permit such research uses.

6.3.2 Virtual or physical data safe rooms (required of researchers)

If research outputs are themselves high-risk, the data must be transferred with encryption either to:

- A virtual clean room environment that meets the requirements outlined in Section 6.3.1, or
- A physical safe room, wherein
    - Access is restricted to authorized personnel,
    - Researchers' activities are monitored and auditable,
    - Data analysis takes place on designated machines that are secured by encryption and disconnected from the internet.

If these specifications cannot be met, the high-risk data must remain within the DSO's secure environment.

Similarly, if research processing is high risk, despite the original data indicating a lower risk category, researchers must either make use of virtual or physical data safe rooms within their own institutions or rely on virtual clean rooms provided by the DSOs for analysis and storage of the research outputs.

Table 4: Safeguards for medium-risk processing (Categories C and B)

Safeguard	Required or Recommended	Researcher Role	Research Institution Role	DSO Role
Virtual clean rooms	Required	Provides required information; accesses under provided conditions	NA	Establishes and oversees
Virtual or physical data safe rooms	Required	Accesses under provided conditions	Establishes and oversees	NA

6.4 Additional safeguards

This Code requires and recommends certain technical and organisational safeguards based on an assessment of current best practices. Other safeguards may be available to researchers and DSOs, and this Code should not be interpreted to prohibit implementation of such safeguards. For example, in certain research contexts, cryptographic technologies such as Private Join and Compute[25] or privacy-

[25] Google Security Blog. (2019) "Helping organizations do more without collecting more data," https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html.

protecting machine learning techniques such as federated learning[26] may be appropriate.

7 Ethical and Methodological Peer Review

Independent review by qualified persons of a research proposal is an important safeguard that does not relate to the risk of data breach. Indeed, research will only qualify under this Code where methodological and ethical reviews have been carried out. Peer review may be organized by the lead individual researcher's institution or rely on an appropriate third-party.

7.1 Ethical review

7.1.1 Panels

Researchers must submit their research proposal – including the DNMP – for ethical review by a panel of at least 3 people with appropriate expertise in the ethics of data-driven research in the field(s) relevant to the research proposal.

Ethical reviewers must be free from any (i) conflicts of interest and (ii) involvement in the Research.

7.1.2 Considerations

Ethical review will be bespoke to the specific project, but is likely to consider:

- Whether, when used, consent procedures are appropriately informative and avoid coercion.
- Whether data for consenting subjects might inadvertently reveal data for non-consenting subjects.
- Whether, when used, deception of subjects is justified and what procedures are needed to mitigate its potential harms.

[26] Google AI Blog. (2017). "Federated learning: Collaborative machine learning without centralized training data," https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

- Whether any considerations apply for special populations, such as children.
- Whether the wage for external task workers (e.g., via Amazon Mechanical Turk) is fair.
- Whether the research might pose harm to the researchers themselves (e.g., for those engaging with hateful or violent content).

This list of considerations is far from exhaustive. When preparing their research proposals and plans, researchers relying on this Code should, as a general rule, follow the *Ethical Guidelines for Internet Research* of the Association of Internet Researchers (AoIR), as well as any other specialized or sector-based guidelines appropriate to the research. (The AoIR guidelines themselves point to other such specialized guidance.) As the AoIR guidelines foreground the understanding that ethical norms are context-dependent and culturally-bound, they are particularly well-suited for consideration and application by researchers operating under the data privacy regimes tied to the GDPR *and* varying Member State laws.

7.2 Methodological review

7.2.1 Panels

Researchers must also submit their research proposal – including the DNMP – for methodological review to a panel of at least [2] people with appropriate expertise in data-driven research methods in the field(s) relevant to the research.

Methodological reviewers must be free from any (i) conflicts of interest and (ii) involvement in the Research. In practice there may well be overlap between the ethical and methodological review panels.

7.2.2 Considerations

Methodological review will evaluate the appropriateness of the methodological approach, including confirming the link between the data needs and the research purpose. The methodological review must focus on evaluating whether:

- The proposed methodologies are broadly suited to achieve the research objectives, answer the research questions, and test the hypotheses, as applicable.

- The researcher(s) involved are qualified to perform the research in question (or the required qualifications in person specifications being used for recruitment are appropriate).

This review process is not intended as a check of methodological minutiae, but must be used to verify that the general methodological approaches are aligned with the intended research outcomes. For example, if a researcher proposes to use topic modelling, reviewers should consider whether (i) topic modelling is appropriate to advance the project's stated aims and (ii) the requested data are appropriate to this methodology, but *not* whether the researcher will apply the latest innovations in topic modelling.

Reviewers should represent, and apply the standards used within, the primary field(s) of study on which the research draws.

7.3 Research institutions' practices

Research institutions will be central to facilitating ethical and methodological review (for example, through the recruitment of qualified peers). They should aim to:

- Streamline the required review processes via a single workflow that avoids duplication wherever possible;

- Permit and enable consolidation of proposals where multiple projects are closely linked; and

- Enable expedited reviews for:

    - Research that presents minimal risk — i.e., projects falling in Category D

- New research projects that vary in minor ways—e.g., based on the topic at hand—from approved projects
- Updates to Data Needs and Management Plans for ongoing projects
- Urgent-need research (e.g., research responding to a public health crisis).

7.4 Certification

Researchers should obtain written certification of approval (forms of certification are provided at Annex 1A and 1B). These certifications can be used to provide assurance to DSOs that the required reviews have been carried out by appropriate institutions.

8 DSO Review

Where DSOs are not joint controllers for the processing carried out by researchers, they will need to be assured that (i) the proposed processing is for qualifying research under this Code, and (ii) that appropriate safeguards for data subjects' rights and freedoms, and technical and organisational measures, are in place to enable them to rely on the research exemptions in the GDPR.

This proposal for a Code aims to limit the amount of information reviewed by DSOs to only what is necessary through:

- Researchers' proposals under the Code focusing on their data practices (through the DNMP) with only a high-level overview of their methodology;
- Certification of ethical & methodological review rather than DSOs engaging in these reviews directly.

In many cases, it will be appropriate for DSOs and researchers to engage in some dialogue about the safeguards to be employed – whether transparency measures or data practices –limited to what is required for the DSO to be assured that the relevant GDPR research exemptions can be relied on. This should promote:

- The maintenance of researchers' independence;
- Timely and administratively streamlined submission and approval of requests for data sharing under the Code; and
- DSO's ability to demonstrate that they are not joint controllers for researchers' processing.

Annex 1A:

CHECKLIST FOR RESEARCHERS: ARE YOU READY TO SUBMIT A REQUEST?

Reviewed relevant Codebook(s) (see Section 2.1); clarified any outstanding questions with DSO contacts	
Assessed risk level of proposed research processing and assigned a risk category (see Section 5)	
Selected and developed a plan for implementation of appropriate safeguards (See Part I and Section 6)	
Prepared a Data Needs and Management Plan (see Section 4) outlining: • Research overview and team • Data needs • Planned safeguards	
Obtained written approval (certification) of DNMP from institution's DPO	
Put proposal through ethical review (see Section 7.1) and received written approval (certification) in the form at Annex 1A	
Put proposal through methodological review (see Section 7.2) and received written approval (certification) in the form at Annex 1B	

Annex 1B:

FORM OF CERTIFICATION FOR ETHICAL REVIEW

[DATE]

To whom it may concern:

This letter certifies that the research proposal titled _____, was submitted to [Committee/Department Name] of [Institution] on [DATE] for review. The [Committee/Institution Name] **approved** that the proposal conforms to accepted ethical standards for data-driven research in the relevant academic field.

Reasons	*Brief outline of reasons for decision and any reservations or conditions on the approval*
Review process	*Brief outline of review process*

[This approval is valid until [DATE], at which point the research project will require supplementary review.] OR [it has been determined this research project does not require continuing review and this approval does not have an expiration date.]

Certified: [APPEND STAMP OR SEAL OF INSTITUTION OR COMMITTEE]

Annex 1C:

FORM OF CERTIFICATION FOR METHODOLOGICAL REVIEW

[DATE]

To whom it may concern:

This letter certifies that the research proposal titled _____, was submitted to [Committee/Department Name] of [Institution] on [DATE] for review. The [Committee/Institution Name] **approved** that the proposal is reasonably designed to achieve its objectives and the proposed methodology accords with recognised standards in the relevant field or area of research.

Reasons	*Brief outline of reasons for decision and any reservations or conditions on the approval*
Review process	*Brief outline of review process*

[This approval is valid until [DATE], at which point the research project will require supplementary review.] OR [it has been determined this research project does not require continuing review and this approval does not have an expiration date.]

Certified: [APPEND STAMP OR SEAL OF INSTITUTION OR COMMITTEE]

Annex 2:

CHECKLIST FOR DSOS: ARE YOU READY TO ENTER A DATA SHARING AGREEMENT?[27]

Codebook that researcher has used to formulate proposal is up to date and accurate (see Section 2.1)	
Reviewed Data Needs and Management Plan, including research institution DPO sign-off (see Section 4)	
Proposed research purpose and field of inquiry and institution meet the requirements set out in the Preamble to the Code	
Raised and resolved questions (if any) about researcher's assessment of risk level and proposed safeguards (see Sections 5 and 6)	
Confirmed your organisation's readiness to implement agreed safeguards (e.g. transparency measures, data practices, access controls etc.) (see Part I of the Code and Section 6)	
Reviewed written confirmation that research proposal has passed ethical and methodological review (see Section 7 and 8)	

[27] This checklist caters to a typical data sharing scenario in which a platform is satisfied that it is not a joint controller for the processing carried out by the researcher.

Annex 3:

Legitimate Interests Assessment Template

Background

To rely on the "legitimate interests" legal basis under Article 6(1)(f) of the GDPR, a controller must meet three cumulative conditions: (1) there must be an identified legitimate interest in the expressed purpose of the processing, (2) the processing of personal data must be necessary for that interest pursued by the researcher or by a third party i.e. the public, and (3) the interest must not be overridden by the rights and interests of affected data subjects. This is known as a legitimate interests assessment (LIA) and should be carried out before the processing has begun. A record of the LIA and the outcome should be recorded and should be kept under review if there is a significant change in the purpose, nature or context of the processing.

If special categories of data are available and intended to be used, additional requirements would apply as per art. 9 GDPR. Data related to criminal offences cannot be processed unless as determined by Member State law as per art. 10 GDPR and are excluded from the scope of this document.

Controllers in the public sector may not rely on legitimate interests where they are performing a task that has been assigned to them by European Union or Member State law. In that case, the public sector controller may instead rely on the "public interests" basis specified in Article 6(1)(e) for such processing.

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing.

1. Legitimate interest (i.e. purpose test)

The researcher must identify a "legitimate interest" in the identified purpose of processing the data. That interest can be the researcher's own interest, a third party's interest, or an interest of the public at large, provided it is (a) a real and present interest, rather than a speculative future interest, (b) lawful, and (c)

sufficiently specific and clearly articulated to be balanced against particular risks to individuals.

Qualifying research can be considered a legitimate interest if it meets the conditions above. The strength of this interest will depend on the value of the specific activity to the researcher, other third parties, and the public, taking into account the relevant, legal, cultural and societal recognition of these interests as legitimate.

Factors to consider:

- Is there a sufficiently specific and limited research purpose?
    - What is the purpose? Why does the researcher want to process the data?
    - The research qualifies as a scientific research
    - The research proposal seeks to address a discrete and articulated research question
    - The research design is limited in time and scope
- Is the research purpose recognized as legitimate within the relevant community(ies)?
    - The research proposal seeks to address a question of scholarly importance in the EU or the EU Member State where the relevant data subjects are located
- What benefit does the researcher expect from the processing?
    - When considering the benefits within a given research project, the GDPR expressly recognizes that research benefits society. For instance, the GDPR acknowledges that within “social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of

social conditions, such as unemployment and education with other life conditions". As a result, "in order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards".

- Has the researcher demonstrated that the research serves a societally beneficial purpose?
- The research does not contravene any EU or Member State laws (including data protection rules, e-privacy legislation and those other than privacy and data protection laws) that apply to the researcher, as well as industry guidelines, codes, and ethical practices.
- The researcher serves an identified and articulated public interest and is not merely for the private benefit of the researcher or other related parties.

2. Necessity

The researcher must evaluate the "necessity" of processing personal data for the purpose of the legitimate interest. The test of necessity in, *inter alia*, Article 6 UK GDPR is well-established as involving a strict approach. Necessity means that the researcher is to assess if "*there are less restrictive measures that can be taken, they should be taken*". Necessity must therefore be approached by objectively considering what is strictly necessary to achieve the objective.

"Necessity" thus requires a strong connection between the proposed activity (i.e., the purpose) and the need to process the requested personal data. Necessity requires the researcher to demonstrate that the data and the way it will be processed is suitable and scientifically justified to conduct the specific research purpose and to consider and rule out less intrusive alternatives for achieving the purported aims.

Factors to consider:

- Has the researcher demonstrated that the data intended to be used are suitable and necessary to conduct the specific research purpose?
    - Will the processing help achieve the purpose? In particular, is access to the data being processed by the DSO necessary to answer the research question
    - The research design requires analysis of the only minimum necessary data categories relating to the minimum number of data subjects to achieve the research purpose
    - The researcher has committed not to use data received for one study[28] for any other study (unless specifically authorized)
- Is the processing proportionate?
    - Can the researcher achieve the same purpose without the processing?
    - Can the same purpose be met by processing less data or by processing the data in another way that has less impact on individuals?
    - Has the researcher demonstrated that other research designs that are less intrusive would be insufficient to achieve, or would detract from achievement of, the research aims?
    - The researcher has considered other research designs that would involve accessing less data and has determined that those designs would be insufficient to answer the proposed question

[28] Researchers will need to consider what constitutes ‘one study’ for their field and work. ‘One study’ is likely more extensive than the work leading to a single publication, however.

3. Balancing test

Finally, the researcher must balance the interests they have identified against the potential risks to the rights and interests of affected data subjects. The companies and the researcher may proceed with the data sharing provided that the data subject rights and interests are not unduly prejudiced by the processing activity.

This analysis must take into account (a) the strength of the relevant interests, (b) the risks for affected data subjects, and (c) the efficacy of proposed safeguards.

Factors to consider:

- What benefits would the proposed study have?
    - Who will benefit from the proposed study?
    - How strong are the potential benefits for the research community and the public?
    - How likely is the research design to realize the potential benefits?
- Do data subjects reasonably expect their data to be processed for this purpose?
    - Will notice of the particular study be provided to data subjects?
    - If not, does the research purpose align with any descriptions and notices provided to data subjects?
    - What is the nature of the relationship with the data subject?
- Nature of the data
    - Will the researcher have access to “special categories of personal data” under art. 9 GDPR or personal data concerning criminal convictions and offenses under art. 10 GDPR?

- Will researchers have access to any information that would be viewed as sensitive (e.g. location/movements, financial information)?
- Will the data permit researchers to make sensitive inferences about data subjects?
- Will the data involve children or other vulnerable people?
- What technical measures will be applied to the data to reduce its identifiability?
- What are the risks that data subjects could be identified from the dataset?

- What is the likely impact and the risks that could arise as a result of the proposed research design?
  - What are the possible impacts on people? In particular, can the researcher identify potential harms that could befall data subjects as a result of the research design?
  - What are the severity and likelihood of those potential consequences?
  - Will data subjects be able to exercise control over the information once it is with researchers?
- What technical and organizational safeguards are in place to protect against the risks (see Section 4 of Part I for further information)?
  - What other technical safeguards will be implemented to protect against the risks (e.g. clean rooms)?
  - What procedural safeguards will apply (e.g. oversight and audit mechanisms)?

- Will data subjects have the ability to opt-out and exercise other data protection rights?
- How effective are these safeguards at preventing or reducing the risks identified above?

- Have any circumstances changed between the DSO and the data subject?
  - Has the data subject withdrawn consent or otherwise objected to processing by the DSO? If so, the data subject's indication of their wishes should be given sufficient weight. In such circumstances, it is unlikely that the researcher could justify the continued processing unless the researcher demonstrates compelling grounds to do so.

Record of decision

Can you rely on legitimate interests for this processing? Do the potential benefits outweigh the potential risks? Or are your legitimate interests outweighed by the risks?	Yes / No
Do you have any comments to justify your answer? (optional)	
Assessment completed by	
Date	

Annex 4 - Compendium of provisions relevant to the sharing of personal data for research purposes in the context of social media platforms

EU[i]	Art.6(4) (purpose limitation – research is compatible)[ii]	Art. 9(2)(j) (opening clause for processing for archival, scientific/ historical research purposes …)[iii]	Art.85 (balancing protection of personal data with freedom of expression and information, including academic expression)[iv]	Art. 89 (safeguards for archiving, scientific/ historical research purposes)[v]	Art. 89 (derogations from data subject rights for processing for scientific/ historical research purposes)[vi]	Other laws	Comment
UK[vii]	N/A	Opening clause used: Processing without consent permitted – ss. 10(1)(e) and 10(2)[viii] and Paragraph 4, Part 1, Schedule 1[ix]	Derogations introduced where required for freedom of expression/ information – s. 15(2)(e)[x] and Para. 26, Part 5 Schedule 2[xi]	Specific safeguards for research purposes set out at ss. 19(1)-(3)[xii]	Derogations from various obligations – ss. 15(2)(f)[xiii] and Para. 27, Part 6, Schedule 2[xiv]	N/A	N/A
Belgium[xv]	N/A	N/A	Derogations for processing for journalistic purposes and for the purposes of academic, artistic or literary expression – Art. 24[xvi]	N/A	Derogations from all obligations listed in Art.89, where derogations are necessary to carry out the research, and subject to additional safeguards [xvii]	N/A	The Belgian legislator, in our view, incorrectly, assumed that Art. 9(2)(j) GDPR did not require implementation under local Belgian law as it assumed that this was not necessary as Art. 89(1) GDPR would be directly applicable. There are indications that this will be rectified, and that work is underway on a legislative amendment that will implement Art. 9(2)(j) GDPR under Belgian law, which may also provide appropriate safeguards for the processing of special categories of personal data for purposes of archiving, scientific, historical research purposes.
Denmark[xviii]	Research can in principle be a secondary purpose provided requirements found in ss. 5(2)[xix] are met (largely a repetition of Art.6(4) requirements)	Opening clause used: Processing without consent permitted for statistical or scientific studies of significant importance to society however, subject to purpose limitation (exemption generally cannot be applied if the processing	Derogations introduced where required for freedom of expression / information and literary works (fiction and non-fiction) – ss. 3(1) and (4)-(8)[xxi]	Data can only be processed for these purposes (subject to purpose limitation. Prior DPA approval required for disclosures to third parties in three particular situations, one of them being where disclosure is for publication in	Absolute derogations from various transparency obligations – s. 22(5)[xxiv]	N/A	The Danish Supervisory Authority ("Datatilsynet") has issued Guidance on the Executive Order no. 1509[xxv], including providing an online form which should be used when applying for approval for disclosure of data to third parties.

Note: this is an A3-sized page. It will not print properly on A4 paper.

EU[i]	Art.6(4) (purpose limitation – research is compatible)[ii]	Art. 9(2)(j) (opening clause for processing for archival, scientific/ historical research purposes …)[iii]	Art.85 (balancing protection of personal data with freedom of expression and information, including academic expression)[iv]	Art. 89 (safeguards for archiving, scientific/ historical research purposes)[v]	Art. 89 (derogations from data subject rights for processing for scientific/ historical research purposes)[vi]	Other laws	Comment
		is also carried out for other/several purposes) – ss. 10(2)-(4)[xx]		a recognised journal ss. 10(3)-(4)[xxii] and subject to responsibilities for the disclosing controller and receiving controller (e.g. pseudonymisation, unless strictly necessary for the research at hand to be able to identify individuals) - Executive Order no. 1509 of 18 December 2019 [xxiii]			
France[xxvi]	N/A	No opening clause used – ss. Art. 6[xxvii]	Derogations introduced where required for freedom of expression/information – ss. Art. 3[xxviii] and Art. 80[xxix]	Specific safeguards for research purposes set out – ss. Art. 78[xxx] and Art. 79[xxxi]	Derogations from various obligations – ss. Art. 116[xxxii] of Decree of application for French Data Protection Law[xxxiii]	Decree of application for French Data Protection Law	There are no specific provisions in French Data Protection Law relevant to the sharing of personal data for research purposes in the context of social media platforms. Therefore, the following provisions refer to the sharing of personal data for research purposes
Germany[xxxiv]	N/A	Opening clause used: Processing without consent permitted – ss. 27 (1)[xxxv], 28 (1)[xxxvi] BDSG	Derogations regarding the publication of research results – s. 27 (4)[xxxvii] BDSG Derogations from various obligations for journalistic purposes – s. 23[xxxviii] MStV, ss. 22[xxxix] and 23[xl] KUG.	Specific safeguards for archiving and research purposes set out at ss. 22 (2), second sentence[xli], 27 (1), second sentence, (3) [xlii], 28 (1), second sentence[xliii] BDSG	Derogations from various obligations – ss. 27 (2)[xliv], 28 (2)-(4)[xlv] BDSG	In context of blocked, removed, or illegal social media content: Obligation for social media networks to report about access by scientists/	The provisions of the NetzDG (see column to the left) specifically relate to platform-to-researcher data sharing. Generally further sector specific derogations may apply (e.g. for the health sector or public institutions), but these are usually less relevant for social media platforms. In Germany there are 16 different federal states with own state laws, which may apply

Note: this is an A3-sized page. It will not print properly on A4 paper.

EU[i]	Art.6(4) (purpose limitation – research is compatible)[ii]	Art. 9(2)(j) (opening clause for processing for archival, scientific/ historical research purposes …)[iii]	Art.85 (balancing protection of personal data with freedom of expression and information, including academic expression)[iv]	Art. 89 (safeguards for archiving, scientific/ historical research purposes)[v]	Art. 89 (derogations from data subject rights for processing for scientific/ historical research purposes)[vi]	Other laws	Comment
						researchers and researcher's right to request certain information (including personal data), - ss. 2 (2) no. 2 and no. 13,[xlvi] 5a[xlvii] NetzDG	in addition to or instead of the cited German federal law, in particular: For research by public institutions of a federal state (e.g. public universities) such state laws may apply (provisions are often similar to the federal BDSG). For journalistic purposes state laws may apply (and include derogations from various obligations, often similar to the MStV[xlviii]).
Ireland[xlix]	N/A	Processing of special category personal data is lawful where processing is necessary and proportionate – ss 54[l]	Exemptions specified where required for the purpose of exercising the right to freedom of expression and information – ss 43[li]	Processing permitted subject to certain safeguards – ss 42 and 36(1)[lii]	Derogations from various obligations – ss 61[liii]	N/A	N/A
Italy[liv]	N/A	Italian Data Protection Code provides a public interest lawful basis for research as set out by other laws – Section 2-e[lv]	Derogation - ss. 136 and 137[lvi] of the Italian Data Protection code	Specific safeguards – ss. 101 and 102[lvii] of the Italian Data Protection Code re: archiving and historical research Third parties can process personal data for scientific research or statistical purposes, without informing the data subject if it proves	Derogation to the right to erasure – ss. 99 and 100[lix] Italian Data Protection Code and section 7[lx] of the Deontological rules for processing for archiving purposes in the public interest or for scientific, or historical research purposes published pursuant to Art.	N/A	N/A

Note: this is an A3-sized page. It will not print properly on A4 paper.

EU[i]	Art.6(4) (purpose limitation – research is compatible)[ii]	Art. 9(2)(j) (opening clause for processing for archival, scientific/ historical research purposes …)[iii]	Art.85 (balancing protection of personal data with freedom of expression and information, including academic expression)[iv]	Art. 89 (safeguards for archiving, scientific/ historical research purposes)[v]	Art. 89 (derogations from data subject rights for processing for scientific/ historical research purposes)[vi]	Other laws	Comment
				impossible, entails a disproportionate effort, or is likely to render impossible, or seriously impair the research. Where data subjects can neither be informed directly *nor* indirectly (e.g. through a newspaper or online notice), this processing can only proceed if authorized by the Italian Data Protection Authority (the "Garante") Section 110-a[lviii]	20(4) of Legislative Decree No. 101 of 10 August 2018		
Luxembourg[lxi]	N/A	Opening clause used: Processing permitted provided that the controller complies with additional safeguards - Art. 64[lxii]	Derogations for journalistic, academic, artistic or literary purposes from data subject rights and from prohibitions or limitations on processing sensitive/judicial data – Art. 62 [lxiii]	Specific safeguards for research purposes – Art. 65 Data Protection Act[lxiv]	Derogations from data subject rights for processing for research purposes – Art. 63 Data Protection Act[lxv]	N/A	N/A
Netherlands[lxvi]	N/A	Opening clause used: Processing without consent permitted, if obtaining explicit consent proves to be impossible or involves a disproportionate effort. In addition, safeguards must be in place to ensure	A balance must be made between the protection of personal data and the protection of the right to freedom of expression. When consent is relied upon as lawful basis, such	N/A	Derogation from various obligations – s. 44[lxix].	N/A	N/A

Note: this is an A3-sized page. It will not print properly on A4 paper.

EU[i]	Art.6(4) (purpose limitation – research is compatible)[ii]	Art. 9(2)(j) (opening clause for processing for archival, scientific/ historical research purposes …)[iii]	Art.85 (balancing protection of personal data with freedom of expression and information, including academic expression)[iv]	Art. 89 (safeguards for archiving, scientific/ historical research purposes)[v]	Art. 89 (derogations from data subject rights for processing for scientific/ historical research purposes)[vi]	Other laws	Comment
		processing is not disproportionate & research must be in public interest. This must be balanced on every concrete case. – s. 24[lxvii]	consent cannot be revoked. – s. 43[lxviii]				
Spain[lxx]	N/A	N/A	New digital right related to freedom of expression and right to rectification on the Internet (article 85)[lxxi]. The tension between privacy and freedom of expression beyond the narrow scope of this digital right is largely dealt with through extensive constitutional case law[lxxii]	N/A	N/A	N/A	N/A

Note: this is an A3-sized page. It will not print properly on A4 paper.

Relevant legal provisions

---

[i] **GDPR** available in English here: 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, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) (europa.eu)

[ii] **Article 6**

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Recital 50

…further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations…

[iii] **Article 9**

[Lawful basis of processing special categories of data]

…

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

[iv] A**rticle 85**

1.Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2.For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.
3.Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

[v] **Article 89**
1.Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

[vi] **Article 89**
2.Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
3.Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
4.Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose,
the derogations shall apply only to processing for the purposes referred to in those paragraphs.

[vii]: **UK Data Protection Act 2018**, available in English here: Data Protection Act 2018 (legislation.gov.uk)

[viii] **Section 10**

Special categories of personal data and criminal convictions etc data

(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the UK GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

…

(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point … (j) of Article 9(2) of the UK GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

[ix] **Schedule 1, Part 1, Para 4**

This condition is met if the processing—
is necessary for archiving purposes, scientific or historical research purposes or statistical purposes;

is carried out in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19), and

is in the public interest.

[x] **Section 15 Exemptions etc**

(2) In Schedule 2—

(e) Part 5 makes provision containing exemptions or derogations from Chapters II, III, IV, and V of the UK GDPR for reasons relating to freedom of expression, (of a kind described in Article 85(2) of the UK GDPR);

[xi] **Schedule 2, Part 5, Para 26**

Journalistic, academic, artistic and literary purposes

(1) In this paragraph, "the special purposes" means one or more of (a) the following—
(a) the purposes of journalism;

(b) academic purposes;

(c)artistic purposes;

(d) literary purposes.

(2) Sub-paragraph (3) applies to the processing of personal data carried out for the special purposes if—
(a) the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material, and

(b) the controller reasonably believes that the publication of the material would-be in the public interest.

(3) The listed UK GDPR provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes.

(4) In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.

(5) In determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of the codes of practice or guidelines listed in sub-paragraph (6) that is relevant to the publication in question.

(6) The codes of practice and guidelines are—
(a) BBC Editorial Guidelines;

(b) Ofcom Broadcasting Code;

(c) Editors' Code of Practice.

…

(9) For the purposes of this paragraph, the listed UK GDPR provisions are the following provisions of the UK GDPR (which may be exempted or derogated from by virtue of Article 85(2) of the UK GDPR)—
(a) in Chapter II of the UK GDPR (principles)—
(i) Article 5(1)(a) to (e) (principles relating to processing);

(ii) Article 6 (lawfulness);
(iii) Article 7 (conditions for consent);
(iv) Article 8(1) and (2) (child's consent);
(v) Article 9 (processing of special categories of data);
(vi) Article 10 (data relating to criminal convictions etc);

(vii) Article 11(2) (processing not requiring identification);

(b) in Chapter III of the UK GDPR (rights of the data subject)—

(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);
(iii) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(iv) Article 16 (right to rectification);
(v) Article 17(1) and (2) (right to erasure);
(vi)Article 18(1)(a), (b) and (d) (restriction of processing);
(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);
(viii) Article 20(1) and (2) (right to data portability);
(ix) Article 21(1) (objections to processing);

(c) in Chapter IV of the UK GDPR (controller and processor)—

(i) Article 34(1) and (4) (communication of personal data breach to the data subject);

(ii) Article 36 (requirement for controller to consult Commissioner prior to high risk processing);

(d) in Chapter V of the UK GDPR (transfers of data to third countries etc), Article44 (general principles for transfers).

[xii] **Section 19**

Processing for archiving, research and statistical purposes: safeguards

(1) This section makes provision about—

(a) processing of personal data that is necessary for archiving purposes in the public interest,

(b) processing of personal data that is necessary for scientific or historical research purposes, and

(c) processing of personal data that is necessary for statistical purposes.

(2) Such processing does not satisfy the requirement in Article 89(1) of the UK GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.

(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.

[xiii] **Section 15**

Exemptions etc

(2) In Schedule 2—

(f) Part 6 makes provision containing derogations from rights contained in Articles 15, 16, 18, 19, 20 and 21 of the UK GDPR for scientific or historical research purposes, statistical purposes and archiving purposes

[xiv] **Schedule 2, Part 6, Paragraph 27**

Research and statistics

(1) The listed UK GDPR provisions do not apply to personal data processed for—

(a) scientific or historical research purposes, or

(b) statistical purposes,

to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.

This is subject to sub-paragraphs (3) and (4).

(2) For the purposes of this paragraph, the listed UK GDPR provisions are the following provisions of the UK GDPR (the rights in which may be derogated from by virtue of Article 89(2) of the UK GDPR)—

(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(b) Article 16 (right to rectification);

(c) Article 18(1) (restriction of processing);
(d) Article 21(1) (objections to processing).

(3) The exemption in sub-paragraph (1) is available only where—
(a) the personal data is processed in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19), and
(b) as regards the disapplication of Article 15(1) to (3), the results of the research or any resulting statistics are not made available in a form which identifies a data subject.

(4) Where processing for a purpose described in sub-paragraph (1) serves at the same time another purpose, the exemption in sub-paragraph (1) is available only where the personal data is processed for a purpose referred to in that sub-paragraph.

Belgian law

[xv] Belgian Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data, available here (in Dutch) and here (in French).

[xvi] **TITLE 1 - PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA**
Chapter V - Processing for journalistic purposes and for the purposes of academic, artistic or literary expression
Art. 24.
(1) The processing of personal data for journalistic purposes shall be understood as the preparation, collection, compilation, dissemination or archiving for the purpose of informing the public, using any media and where the controller undertakes to comply with journalistic deontological rules.
(2) Articles 7 to 10, 11.2, 13 to 16, 18 to 20 and 21.1 of the GDPR shall not apply to the processing of personal data for journalistic purposes and for the purposes of academic, artistic or literary expression.
(3) Articles 30(4), 31, 33 and 36 of the GDPR shall not apply to the processing of personal data for journalistic purposes and for the purpose of academic, artistic or literary expression when such application would compromise an intended publication or constitute a control measure prior to the publication of an article.
(4) Articles 44 to 50 of the GDPR shall not apply to the transfer of personal data carried out for journalistic purposes and the purposes of academic, artistic or literary expression to third countries or international organisations to the extent necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

(5) Article 58 of the GDPR shall not apply to the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression if its application would reveal indications as to the sources of information or constitute a control measure prior to the publication of an article.

[xvii] **TITLE 4 - PROCESSING FOR ARCHIVING IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH OR STATISTICAL PURPOSES AS REFERRED TO IN ARTICLE 89(2) AND (3) OF THE GDPR**

Chapter I. - General Provisions

This Title lays down the exception regime with respect to the rights of data subjects referred to in Article 89 §§ 2 and 3 of the GDPR.

To the extent that the exercise of the rights referred to in Article 89(2) and (3) of the GDPR risks rendering impossible or seriously impeding the carrying out of processing for archiving purposes in the public interest, for scientific or historical research or for statistical purposes, and derogations are necessary to achieve these purposes, these derogations shall be applied under the conditions laid down in this Title.

Art. 187. Articles 190 to 204 [see below] shall not apply subject to compliance with a code of conduct approved in accordance with Article 40 of the GDPR.

Article 188. For the purposes of this Title, the following definitions shall apply:

1° "third party trustee" means the natural or legal person, the de facto association or the public administration, other than the controller for archiving or research or statistical purposes, who pseudonymises the data;

2° "communication of data": communication of data to identified third parties

3° "dissemination of data": publication of data, without identification of the third party.

Art. 189. This Title shall not apply to processing operations carried out by the authorities referred to in Title 3 [Public authorities, excluding law enforcement].

Chapter II. - General Guarantees

Art. 190. The controller shall appoint a data protection officer if the processing of personal data is likely to constitute a high risk as referred to in article 35 of the GDPR.

Art. 191. Prior to collection, and without prejudice to Articles 24 and 30 of the GDPR, the controller shall add the following elements to the register of processing activities for scientific or historical research or statistical purposes:

1° the justification for the use of the data, whether or not pseudonymised

2° the reasons why the exercise of the rights of the data subject threatens to make the achievement of the purposes impossible or to seriously hinder them;
3° where appropriate, the data protection impact assessment when the controller is processing sensitive data, within the meaning of Article 9.1 of the GDPR, for scientific or historical research or statistical purposes.

Article 192. Prior to collection, and without prejudice to Articles 24 and 30 of the GDPR, the controller shall add the following elements to the register of processing activities for archiving in the public interest:
1° the justification of the public interest of the archives preserved;
2° the reasons why the exercise of the rights of the person concerned threatens to make the achievement of the purposes impossible or seriously impede them.

Chapter III. - Data Collection

Section 1. - Collection of data from the data subject

Art. 193. Without prejudice to Article 13 of the GDPR, the controller who collects personal data from the data subject shall inform him of:
1° the fact that the data will or will not be anonymised
2° the reasons why the exercise of the data subject's rights threatens to make the achievement of the purposes impossible or seriously impede them.

Section 2. - Further processing of data

Art. 194. When personal data have not been collected from the data subject, the controller shall enter into an agreement with the person responsible for the original processing.
The first paragraph shall not apply if:
1° the processing relates to personal data that have been made public;
2° when European Union law, a law, a decree or an ordinance:
a) mandates the controller to process personal data for archiving in the public interest, scientific or historical research or statistical purposes; and
b) prohibits the re-use of the collected data for other purposes.
In case of exemption from the conclusion of an agreement, the controller shall inform the controller of the original processing of the data collection.

Art. 195. The agreement or the notification referred to in article 194 shall contain the following elements:
1° in the event of an agreement, the contact details of the controller of the original processing and of the controller of the further processing;
2° the grounds on which the exercise of the rights of the data subject threatens to make the achievement of the purposes impossible or seriously impede them.

Art. 196. The agreement or the notification concerning the data collection shall be attached to the register of processing activities.

Art. 197. The controller shall use anonymous data for research or statistical purposes.
If it is not possible to achieve the research or statistical purpose by processing anonymous data, the controller shall use pseudonymised data.
If it is not possible to achieve the research or statistical objective by processing pseudonymised data, the controller shall use data that have not been pseudonymised.

Section 3. - Anonymisation or pseudonymisation of data processed for scientific or historical research or statistical purposes

Art. 198. When processing data for scientific or historical research or statistical purposes, based on a collection of data from the data subject, the controller shall proceed to anonymise or pseudonymise the data after their collection.

Art. 199. When data are processed for scientific or historical research or statistical purposes by a controller who is the same as the controller of the original processing, the controller shall anonymise or pseudonymise the data prior to their further processing.
The controller may only pseudonymise data if this is necessary for research or statistical purposes, and, if applicable, after having obtained the opinion of the Data Protection Officer.

Art. 201. Without prejudice to special provisions, when data are processed for scientific or historical research or statistical purposes by a controller who is different from the controller of the original processing, the controller of the original processing shall pseudonymise or anonymise the data prior to their communication to the controller of the further processing.
The person responsible for further processing shall not have access to the keys of the pseudonymisation.

Art. 202. (1) Without prejudice to special provisions, in the case of data processing for scientific or historical research purposes, or statistical purposes involving several original processing operations, the persons responsible for the original processing operations shall have the data anonymised or pseudonymised by one of the persons responsible for the original processing operation or by a third party trustworthy person prior to communicating the data to the person responsible for further processing.
(2) Without prejudice to special provisions, in the case of data processing for scientific or historical research purposes or for statistical purposes which links several original processing operations, at least one of which involves sensitive data, the persons responsible for the original processing operations shall, prior to communicating the data to the person responsible for further processing, have the data rendered anonymous or pseudonymised by the person responsible for the original processing of sensitive data or by a third party trustworthy person.
Only the controller of the original processing who has pseudonymised the data or the third-party trustee shall have access to the pseudonymisation keys.

Art. 203. The third-party fiduciary is:
1° subject to professional secrecy in the sense of article 458 of the Penal Code, subject to other provisions of this Law and of the GDPR;
2° not dependent on the person responsible for the initial and further processing.

Art. 204. If a Data Protection Officer has been appointed in accordance with Article 190, he or she shall provide advice on the use of the various methods of pseudonymisation and anonymisation, in particular their effectiveness in terms of data protection.

Section 4. - Dissemination of data processed for archiving in the public interest, scientific or historical research or statistical purposes

Art. 205. Without prejudice to the European regulations, special laws, ordinances and decrees that impose stricter conditions on the dissemination of data processed for archiving in the public interest, scientific or historical research or statistical purposes, the controller shall not disseminate non-pseudonymised data unless:
1° the data subject has given his/her consent; or
2° the data have been made public by the data subject himself; or
3° the data are closely connected with the public or historical character of the person concerned; or
4° the data are closely connected with the public or historical nature of facts in which the person concerned was involved.

Art. 206. Without prejudice to the European regulations, special laws, ordinances and decrees that impose stricter conditions on the dissemination of data processed for archiving in the public interest, scientific or historical research or statistical purposes, the controller may disseminate pseudonymised personal data, except as regards the personal data referred to in Article 9.1 of the GDPR.

Section 5. - Communication of data processed for archiving in the public interest, scientific or historical research or statistical purposes

Art. 207. Without prejudice to European Union law, special laws, ordinances and decrees imposing stricter conditions on the communication, the controller who communicates non-pseudonymised data to an identified third party for the purposes referred to in Article 89 of the GDPR shall ensure that the identified third party cannot reproduce the communicated data, except in handwritten form, if:
1° it concerns personal data referred to in articles 9.1 and 10 of the GDPR; or
2° the agreement between the person responsible for the original processing and the person responsible for the further processing so prohibits; or
3° such reproduction may jeopardise the security of the data subject.

Art. 208. The obligation referred to in Article 207 shall not apply if:
1° the data subject has given his/her consent; or
2° the data have been made public by the person concerned; or
3° the data are closely linked to the public or historical nature of the person concerned; or
4° the data are closely connected with the public or historical nature of facts in which the person concerned was involved.

Danish Law

[xviii] **Danish Data Protection Act** (Act No. 502 of 23 May 2018), available in Danish here: Databeskyttelsesloven. Available in English here (please note that only the Danish version of the text has legal validity): Danish Data Protection Act.

[xix] **Section 5**
Danish Data Protection Act
(1) Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

(2) To ascertain whether processing for another purpose is compatible with the purpose for which the personal data were originally collected, see subsection 1, the data controller shall according to Article 6(4) of the General Data Protection Regulation take into account aspects such as:

1) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
2) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
3) the nature of the personal data, in particular whether special categories of personal data are processed, see Article 9, or whether personal data related to criminal convictions and offences are processed, see Article 10;
4) the possible consequences of the intended further processing for the data subjects; and
5) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

(3) Regardless of subsections (1) and (2), in consultation with the Minister of Justice and within the scope of Article 23 of the General Data Protection Regulation, the competent minister may lay down more detailed rules to the effect that public authorities may further process personal data for another purpose than that for which they were originally collected, irrespective of the compatibility of the purposes. The first sentence of this subsection shall not apply to the processing of data pursuant to section 10. In respect of health data and genetic data mentioned in Article 9(1) of the General Data Protection Regulation that have been collected pursuant to section 7(3) of this Act or under Danish healthcare legislation, the first sentence of this subsection shall only apply to the extent that the purpose of the further use of these data is compatible with the purpose for which these personal data were originally collected.

[xx] **Section 10**

Danish Data Protection Act

(1) Data as mentioned in Article 9(1) and Article 10 of the General Data Protection Regulation may be processed where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant importance to society and where such processing is necessary in order to carry out these studies.

(2) The data covered by subsection (1) may not subsequently be processed for other than scientific or statistical purposes. The same shall apply to processing of other data carried out solely for statistical or scientific purposes under Article 6 of the General Data Protection Regulation.

(3) The data covered by subsections (1) and (2) may only be disclosed to a third party with prior authorisation from the supervisory authority when such disclosure:

1) is made for the purpose of processing outside the territorial scope of the General Data Protection Regulation, see Article 3 of the General Data Protection Regulation;

2) relates to biological material; or

3) is made for the purpose of publication in a recognised scientific journal or similar.

(4) The supervisory authority may lay down general terms for the disclosure of data covered by subsections (1) and (2), including for disclosure that does not require authorisation under subsection (3). The supervisory authority may further lay down more detailed terms for the disclosure of data under subsection (3).
(5) Irrespective of subsection (2), in consultation with the Minister of Justice, the Minister of Health may lay down rules to the effect that data covered by subsections (1) and (2) which have been processed for the purpose of carrying out statistical and scientific healthcare studies may subsequently be processed for other than scientific or statistical purposes where such processing is necessary for safeguarding the vital interests of the data subject.

[xxi] **Section 3**

Danish Data Protection Act

(1) This Act and the General Data Protection Regulation shall not apply where this will be contrary to Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms or Article 11 of the EU Charter on Fundamental Rights.
(4) This Act and the General Data Protection Regulation shall not apply to the processing of data covered by the Act on information databases operated by the mass media.
(5) This Act and Chapters II-VII and IX of the General Data Protection Regulation shall not apply to information databases that exclusively include already published periodicals or sound and image programmes covered by paragraph 1 or 2 of section 1 of the Media Liability Act, or parts thereof, provided the data are stored in the information database in the original version published. However, the provisions of Articles 28 and 32 of the General Data Protection Regulation shall apply.
(6) This Act and Chapters II-VII and IX of the General Data Protection Regulation shall not apply to information databases that exclusively include already published texts, images and sound programmes covered by paragraph 3 of section 1 of the Media Liability Act, or parts thereof, provided the data are stored in the information database in the original version published. However, the provisions of Articles 28 and 32 of the General Data Protection Regulation shall apply.
(7) This Act and Chapters II-VII and IX of the General Data Protection Regulation shall not apply to manual files of cuttings from published, printed articles exclusively processed for journalistic purposes. However, the provisions of Articles 28 and 32 of the General Data Protection Regulation shall apply.
(8) This Act and Chapters II-VII and IX of the General Data Protection Regulation shall not apply to the processing of data that otherwise takes place exclusively for journalistic purposes. However, the provisions of Articles 28 and 32 of the General Data Protection Regulation shall apply. The first and second sentences shall also apply to the processing of data for the sole purpose of artistic or literary expression [*this includes fiction and non-fiction, we note that it is a fine line between non-fiction and some academic research and this would be open to debate depending on the circumstances of the research]*.

[xxii] **Section 10**

Danish Data Protection Act

(1) Data as mentioned in Article 9(1) and Article 10 of the General Data Protection Regulation may be processed where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant importance to society and where such processing is necessary in order to carry out these studies.

(2) The data covered by subsection (1) may not subsequently be processed for other than scientific or statistical purposes. The same shall apply to processing of other data carried out solely for statistical or scientific purposes under Article 6 of the General Data Protection Regulation.

(3) The data covered by subsections (1) and (2) may only be disclosed to a third party with prior authorisation from the supervisory authority when such disclosure:

1) is made for the purpose of processing outside the territorial scope of the General Data Protection Regulation, see Article 3 of the General Data Protection Regulation;

2) relates to biological material; or

3) is made for the purpose of publication in a recognised scientific journal or similar.

(4) The supervisory authority may lay down general terms for the disclosure of data covered by subsections (1) and (2), including for disclosure that does not require authorisation under subsection (3). The supervisory authority may further lay down more detailed terms for the disclosure of data under subsection (3).

(5) Irrespective of subsection (2), in consultation with the Minister of Justice, the Minister of Health may lay down rules to the effect that data covered by subsections (1) and (2) which have been processed for the purpose of carrying out statistical and scientific healthcare studies may subsequently be processed for other than scientific or statistical purposes where such processing is necessary for safeguarding the vital interests of the data subject.

[xxiii] **Executive Order no. 1509 of 18-12-2019 on the disclosure of personal data covered by the Data Protection Act, section 10, subsection 1 and 2 (English Translation)** The Danish language version is available here: BKG 1509

Chapter 1 Scope of application

Section 1.

The Act applies to the disclosure of personal data covered by Section 10(1) and (2) of the Danish Data Protection Act, cf. however Subsection 2.

Subsection 2. The Act does not apply if the Danish Data Protection Agency has set conditions for disclosure pursuant to the Danish Data Protection Act Section 10(4)(2)

Chapter 2 The Obligations of the Data Controller Providing Information

Section 2. Personal data may only be disclosed when it is necessary for the data controller receiving information to carry out statistical or scientific studies of significant societal importance.
Subsection 2. Data may not later be processed for any other reason than scientific or statistical purposes.
Subsection 3. If the data controller providing the information has informed the data subject that the data will not be disclosed, no disclosure may be made.

Section 3. Disclosure of personal data must be done in pseudonymised form, so that the information is not directly attributable to the data controller receiving information, cf. however Section 4.

Section 4. If it is absolutely necessary to identify the individual data subject in order to carry out the statistical or scientific study, supplementary information may be disclosed so that the personal data can be attributed to specific physical persons.
Subsection 2. To the greatest extent possible, the additional information must be disclosed separately from the personal data to an authorised person at the data controller receiving the data, cf. Section 10.

Section 5. If the personal data is disclosed when transferred over the Internet or other external network, the data controller providing the data must take appropriate security measures.
Section 6. When transmitting confidential and sensitive personal data over the Internet or external networks, the data controller must, at minimum, use appropriate encryption.

Section 7. In accordance with Article 32 of the General Data Protection Regulation, appropriate technical and organisational measures must be implemented, taking into account the current technical level, implementation costs and the nature, scope, context and purpose of the processing in question, as well as the risks of varying probability and seriousness of the rights and freedoms of natural persons in order to ensure a level of security that corresponds to these risks.

Section 8. Before disclosure, it must be ensured that the personal data is only used for statistical or scientific studies. It must also be ensured that the receiving data controller complies with Sections 10-14.

Section 9. From the time of disclosure, documentation must be provided showing that Section 8 has been complied with. Documentation must take the form of obtaining a written based statement or similar from the data controller receiving the data.

Chapter 3 The receiving data controller

Section 10. Disclosure must be done to persons who are authorised to have access to the personal data in question by the data controller receiving the data. Only persons who actively work with personal data may be authorised. The individual persons may not be authorised for uses that they do not need.

Section 11. The necessary instructions must be given to the employees who have access to the personal data. In regard to this, the employees must be made aware that the personal data may only be processed for the purpose of carrying out statistical or scientific studies and that the personal data may not later be processed for anything other than scientific or statistical purposes.

Section 12. No more information than is necessary for the purpose of carrying out the statistical or scientific study may be processed. Upon receipt of the data, personal data not necessary for the purpose of the statistical or scientific study must be deleted, destroyed or returned as soon as possible.

Section 13. In accordance with Article 32 of the General Data Protection Regulation, appropriate technical and organisational measures must be implemented, taking into account the current technical level, implementation costs and the nature, scope, context and purpose of the processing in question, as well as the risks of varying probability and seriousness of the rights and freedoms of natural persons in order to ensure a level of security that corresponds to these risks.

Section 14. Personal data must be deleted, anonymised, destroyed or returned at the end of the study, so that it is subsequently not possible to identify natural persons based on the information or in combination with other information. Alternatively, personal data may be transferred for storage in the archive, in accordance with the rules in the archive legislation.

Chapter 4 Penalty

Section 15. Unless a higher penalty is inflicted under the other legislation, a violation of Sections 2-9 is punishable by a fine or imprisonment for up to 6 months.

[xxiv] **Section 22**

Danish Data Protection Act - Restrictions of the rights of data subjects

(5) Articles 15, 16, 18 and 21 of the General Data Protection Regulation shall not apply if the processing of data takes place exclusively for scientific or statistical purposes.

[xxv] **Guidance on Executive Order no. 1509 of 18-12-2019 on the disclosure of personal data covered by the Data Protection Act, section 10, subsection 1 and 2 (English translation)** The Danish language version is available here: Vejledning til BKG 1509.

Chapter 1 Scope of application

Section 1: The Executive Order applies to the disclosure from a data controller ("the data controller who is providing the data") that has collected and processed personal data for statistical or scientific purposes, pursuant to Section 10(1) of the Data Protection Act and Article 6(1)(e) of the General Data Protection Regulation, to another data controller ("the data controller who is receiving the data") who will also in future process the data for statistical or scientific purposes.

The scope of the Executive Order therefore corresponds to the scope of the Data Protection Act Section 10(2), which states that data processed under Section 10(1) of the Data Protection Act may not later be processed for anything other than statistical or scientific purposes. The same applies to the processing of other data that is only performed for statistical or scientific purposes under Article 6 of the General Data Protection Regulation.

In the Danish Data Protection Act, "Disclosure" is understood as being a transfer to a new independent data controller. The Executive Order therefore does not apply to the transfer of data to a data processor or for further processing internally by the data controller. In these cases, however, the purpose limitation in Section 10(2) of the Data Protection Act continues to apply.

The compliance of the data controller providing the information with the Executive Order must be documented, for example in the form of procedure descriptions and authorisation procedures. The documentation of the data controller's compliance with the Executive Order is regulated separately in Sections 8 and 9. In addition, matters not covered by the Executive Order will be regulated by the general rules in the General Data Protection Regulation and the Data Protection Act for certain data controllers. This applies, for example, to the receiving data controller's processing of personal data after the disclosure.

Chapter 2 The Providing Data Controller's Obligations

Section 2: Personal data may only be disclosed when it is necessary for the data controller receiving the data to carry out statistical or scientific studies of significant societal significance.

Subsection 2. Data may not later be processed for any other purpose than scientific or statistical purposes.
Subsection 3. If the data controller has informed the data subject that the data will not be disclosed, no disclosure may be made.

Section 2(1) of the Executive Order repeats the principle of data minimisation in connection with assessing which personal data will be disclosed.

Subsection 1 means that the data controller submitting the report must make an initial assessment of what personal data is required for the data controller's statistical or scientific investigation.

The data controller must be able to document that a decision has been made on the scope of the disclosure and that this has not been done without initial consideration. The data controller providing the data should clarify the extent to which disclosure is required in cooperation with the data controller receiving it before the disclosure takes place. Reference is also made to the separate assessment to be made pursuant to Section 4.

For example, the Danish Data Protection Agency will not regard Section 2, Subsection 1, as being fulfilled if the disclosure includes personal data about criminal offences, after the receiving data controller has stated that the study relates exclusively to the correlation between the postal code and health conditions.

Section 2(1), must be read in the context of Section 12, as the terms both represent the principle of data minimisation in Article 5(1)(c) of the General Data Protection Regulation. According to Section 2(1), the data controller who is providing the data will be granted considerable leeway in the type of information that may be disclosed at the initial stage of the scientific or statistical study based on the dialogue with the data controller receiving it. Section 12 of the Executive Order will then call for a more detailed, ongoing assessment of the data required by the data controller who is receiving the data after the disclosure.

Section 2(2) of the Executive Order reflects the limitation of purpose in Section 10(2). Section 2(2), can be read in connection with Section 8.

Firstly, the purpose limitation means that processing, including disclosure, can only take place based on legal authority to process data under Article 6(1)(e) of the General Data Protection Regulation for statistical or scientific purposes, and Article 10(1) of the Data Protection Act. This excludes, among other things, the use of personal data for specific case processing or marketing to data subjects.

Secondly, the purpose limitation means that the data controllers may not subsequently process personal data, including the disclosing of such, for any purpose other than scientific or statistical, by obtaining the data subjects' consent to further processing for the new purpose. If the data controller wishes to carry out this type of further processing, the personal data from the data subjects will need to be re-collected, or collected from the original register based on the new legal basis.

Deviations from the limitation of the purpose may be determined in accordance with Section 10(5) of the Data Protection Act, after which the Minister of Health, following a consultation with the Minister of Justice, may establish rules that information covered by Subsections 1 and 2 which has been processed in order to conduct health-care statistical and scientific studies may later be processed for purposes other than statistical or scientific purposes, if the processing is required to safeguard the vital interests of the data subject. The option of establishing such rules has not yet been used.

It is also assumed in Section 14 of the Data Protection Act that transfer to an archive can always take place if the conditions in the archive legislation are met. The transfer to an archive, for example the National Archives, will not be covered by the terms.

The purpose of Section 2(3) of the Executive Order is to ensure, as far as possible, that the data controller does not disclose personal data to a greater extent than the data subject could rightfully expect.

The provision applies only if the data controller has explicitly informed the data subject that no disclosure will take place.

The disclosure may thus still take place if the person registered has not received any information about the disclosure at all, for example, because at the time of collection, the data controller was not aware that the disclosure would actually take place or because the data subject was not notified that the data controller was collecting personal data, for example, because the exception in Article 14(5)(b) of the General Data Protection Regulation was used.

The disclosure can also take place if the data subject has been informed that disclosure will be made to one or more other specific data controllers and it later turns out that it is also relevant to disclose to the receiving data controller.

The ban is thus first and foremost relevant if collection of information from the data subject has been performed and the data subject has been informed pursuant to Article 13 of the General Data Protection Regulation. The disclosure cannot, for example, take place if the data controller, when notifying that data collection is being done pursuant to

Article 13 of the General Data Protection Regulation, has informed the data subject that personal data will only be processed by “the undersigned” or equivalent wording.

Thus, the data controller must make a specific assessment as to whether the data subject has been given a legitimate expectation that no disclosure of personal data about this would occur.

Section 3: Disclosure of personal data must be done in pseudonymised form, so that the information is not directly attributable to the data controller, cf. however Section 4.

The purpose of Section 3 of the Executive Order is to limit the risks to the rights of the data subject resulting from the extensive access to personal data disclosed for statistical or scientific purposes. The provision thus establishes that, as a rule, pseudonymisation must always take place before the disclosure takes place, cf. however, Section 4.

The decisive factor for pseudonymisation to be considered to have occurred is that the data subject can no longer be identified immediately and directly by the recipient.

Pseudonymisation may consist of personal names, personal identification numbers, addresses and other personal data that can be used to immediately and directly identify individuals, transferring it to a separate document ("the additional information"). The separated information can then be replaced in its original context by codes ("the pseudonymised information").

Pseudonymising may be sufficient even if someone who already knows the information – for example the data subject’s family or the data controller who originally provided the information to the data controller – can identify the person to whom the information relates.

Pseudonymisation is not the same as anonymisation in the data protection laws. The latter means that irrevocable deletion has taken place of the information that enables the identification of individuals. Processing of anonymised data is not covered by the General Data Protection Regulation, cf. Article 2(1) of the Regulation.

Section 4: If it is absolutely necessary to identify the individual data subject in order to carry out the statistical or scientific study, supplementary information may be disclosed so that the personal data can be attributed to specific physical persons.
Subsection 2. To the greatest extent possible, the additional information must be disclosed separately from the personal data to an authorised person at the data controller receiving the data cf. Section 10.

The purpose of Section 4(1) of the Executive Order is to ensure that Section 3 does not hinder free research, as it makes an exception to the general rule on the disclosure of pseudonymised information.

The additional information will be only be disclosed to enable the data controller receiving the data to identify individuals immediately and directly if this is strictly necessary for the purpose of the scientific or statistical study. This also applies if pseudonymisation is not feasible in practical terms.

Similarly, in regard to this assessment, the data controller providing the data must, pursuant to Section 2, perform a joint, specific and separate assessment of the necessity of the additional information for the study/further processing with the data controller who is receiving the data.

This will require additional information to be disclosed, if the study cannot go ahead with the pseudonymised information alone, for example if the reason for disclosing the information is to add to and improve other information about the data subjects.

Conversely, the disclosure of additional information for purely pragmatic purposes will not be sufficient, as pseudonymisation entails a considerable use of resources.

Section 4(2) of the Executive Order serves to ensure the rights of the data subject by requiring a separate security measure when disclosing the additional information.

The separation of the additional information from the pseudonymised information must be effective. For example, it is not sufficient for the information to appear in two different places in the same document.

It should also be ensured that the group that has access to the additional information is, as far as possible, limited to a narrower group of people than the group that otherwise has access to the pseudonymised information.

Section 5: If the personal data is disclosed when transferred over the Internet or other external network, the data controller providing the data shall take appropriate security measures.

Section 6: When transmitting confidential and sensitive personal data over the Internet or external networks, the data controller shall, at minimum, use appropriate encryption.

Sections 5 and 6 of the Executive Order emphasise the need for measures to address the specific risks arising from a transfer over external networks over which the releasing and receiving data controllers do not have control.

When transferring confidential and sensitive personal data over the Internet or external networks, the data controllers should refer to the Danish Data Protection Agency's guideline statement on encryption.

Section 7: In accordance with Article 32 of the General Data Protection Regulation, appropriate technical and organisational measures must be implemented, taking into account the current technical level, implementation costs and the nature, scope, context and purpose of the processing in question, as well as the risks of varying probability and seriousness of the rights and freedoms of natural persons in order to ensure a level of security that corresponds to these risks.

Section 7 of the Executive Order repeats the requirement that the data controller providing the data must always carry out a risk assessment through processing, including disclosure, of personal data. The data controller will usually be able to prepare a general risk assessment for the processing of personal data covered by the Executive Order, as both the category of personal data and the nature of the processing will be uniform. In this regard, the Executive Order must be regarded as a minimum requirement, where the providing data controller's risk assessment can lead to further technical and organisational measures being taken.

Section 8: Before disclosure, it must be ensured that the personal data is only used for statistical or scientific studies. It must also be ensured that the receiving data controller complies with Sections 10-14.

The purpose of Section 8 of the Executive Order is to ensure that the data controller providing the data provides information, and the data controller receiving it agrees to the purpose limitation in Section 10(2) of the Data Protection Act and the Executive Order before the disclosure takes place.

As a starting point, it will be sufficient to use the data controller's statement as a basis, as in all circumstances, the receiving data controller will be obligated by the General Data Protection Regulation, unless the disclosure requires the Danish Data Protection Agency's permission under the Danish Data Protection Act Section 10(3)(1), where the Data Protection Agency lays down special terms.

At a minimum, the providing data controller will be required to be informed and receive confirmation that the receiving data controller is aware of the contents of the Executive Order, cf. including Section 9. In cases where the receiving

data controller is covered by the Data Protection Act, cf. Data Protection Act Section 4, it will be sufficient for the providing data controller to disclose this.

The data controller providing the data is not obligated under Section 8 after the disclosure has taken place, cf. however, Section 9 on the documentation obligation. Hence, the data controller providing the data is not responsible for the receiving data controller's failure to comply with the data protection rules and is not obligated to carry out subsequent investigations of the receiving data controller's processing of personal data.

Section 9: From the time of disclosure, documentation must be provided showing that Section 8 has been complied with. Documentation must take the form of obtaining a written based statement or similar from the data controller receiving the data.

Section 9 of the Executive Order must ensure that, after the disclosure has taken place, the data controller submitting the disclosure can document that the disclosure has taken place in accordance with Section 8, including that the data controller receiving it had agreed to Section 10(2) of the Data Protection Act and the Executive Order.

This means that, at the time of disclosure, there must be a dated and written reasoned declaration or the equivalent from the receiving data controller, confirming compliance with the Executive Order's Sections 10-14 and confirming that the information will only be processed for scientific or statistical studies.

The documentation may also include the considerations and examinations, including relevant discussions with the data controller receiving the data that have been conducted in connection with the disclosure.

As a result of Section 41(7) of the Danish Data Protection Act on Limitations, the requirement for documentation will cease no later than after five years. However, after a specific assessment the requirement may cease earlier, for example if the receiving data controller's investigation has been completed shortly after disclosure, and the information has been deleted or equivalent, cf. Section 14.

Chapter 3 The Receiving Data Controller

Section 10: Disclosure must be done to persons who are authorised to have access to the personal data in question by the data controller receiving the data. Only persons who actively work with personal data may be authorised. The individual persons may not be authorised for uses that they do not need.

Section 10 is intended to ensure that only persons who need to use the personal data are authorised to do so and that unauthorised persons do not gain access to the personal data.

Authorisation can be any formal authorisation scheme and workflow set up by the receiving data controller.

The receiving data controller must, as a result of the statistical or scientific study, have determined which persons need to use the personal data and to what extent they have this need. As a result of this, the receiving data controller may grant individuals differentiated access to the personal data according to the individual needs.

If the receiving data controller is only one person, the provision has no particular significance.

Section 11: The necessary instructions must be given to the employees who have access to the personal data. In this regard, the employees must be made aware that the personal data may only be processed for the purpose of carrying out statistical or scientific studies and that the personal data may not be processed later for anything other than scientific or statistical purposes.

The purpose of Section 11 of the Executive Order is to ensure that all employees authorised by the receiving data controller under Section 10 are able to process the data in accordance with the data protection rules.

The necessary instruction may be in the form of ongoing training, instruction and answers to employees' questions about data security.

In this regard, the relevant employees must be made aware of the contents of the Executive Order and the data protection rules in general.

Please refer to the Danish Data Protection Agency’s guidelines on processing security Section 3.3.5. The use of data processors is not covered by the provision and is independently regulated in Article 28 of the General Data Protection Regulation.

Section 12: No more information than is necessary for the purpose of carrying out the statistical or scientific study may be processed. Upon receipt of the data, personal data not necessary for the purpose of the statistical or scientific study must be deleted, destroyed or returned as soon as possible.

The purpose of Section 12 of the Executive Order is to ensure that the principle of data minimisation and the principle of storage limitation are safeguarded after the disclosure has taken place.

The receiving data controller must therefore perform an ongoing assessment of what information is necessary for the conduct of the study and delete information that is unnecessary. Please refer to the instructions for Section 2(1).

When determining that certain information is no longer necessary for the conduct of the study, reference is made to the receiving data controller to the guidelines for Section 14.

Section 13: In accordance with Article 32 of the General Data Protection Regulation, appropriate technical and organisational measures must be implemented, taking into account the current technical level, implementation costs and the nature, scope, context and purpose of the processing in question, as well as the risks of varying probability and seriousness of the rights and freedoms of natural persons in order to ensure a level of security that corresponds to these risks.

Section 13 repeats the requirement for a risk assessment in connection with the data controllers receiving the information provided.

We generally refer to the Danish Data Protection Agency's guidelines on processing security.

Section 14: Personal data must be deleted, anonymised, destroyed or returned at the end of the study, so that it is subsequently not possible to identify natural persons based on the information or in combination with other information. Alternatively, personal data may be transferred for storage in the archive according to the rules in the Danish archive legislation.

It follows from the general principles of data protection that any processing of personal data shall cease when it is no longer necessary for the explicitly stated purpose of the processing.

As the processing covered by the Executive Order is done for the purpose of carrying out a statistical or scientific study, the conclusion of this study will result in the processing being discontinued. This means that the receiving data controller must delete, anonymise, destroy or, if required, return all personal data that it possessed as a result of the disclosure. To the extent that the archive legislation applies, transfer may also take place for storage in the archive.

A statistical or scientific study will be considered to be completed when there is no longer a specific and objective purpose for the processing. However, the provision does not necessitate deletion, etc. at the end of individual stages of the study, cf. however, Section 12. The provision also does not exclude that, during a statistical or scientific study, new questions of a statistical or scientific nature may arise that those involved may wish to delve deeper into during the study or that, as part of the study, they may wish to follow up on the preliminary results in the future, for example, with the aim of investigating a later development in the results of the study.

Being able to keep the personal data for a hypothetical, future statistical or scientific study will not be considered a concrete, objective purpose.

Chapter 4 Penalty

Section 15: Unless a higher penalty is inflicted under the other legislation, a violation of Sections 2-9 is punishable by a fine or imprisonment for up to 6 months.

The data controller's breach of the Executive Order may be punishable by law.

If the receiving data controller violates the provisions of Sections 10-14, they can be punished for violation of the General Data Protection Regulation or the Danish Data Protection Act, cf. Section 41 of the Act.

French Law

[xxvi] : French Data Protection Law: French Data Protection Law, No. 78-17, 6 January 1978

Title 1 Chapter 1 Principles and Definitions

[xxvii] **Article 6**

I. It is prohibited to process personal data revealing the alleged racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of a natural person, or to process genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person.

II. Exceptions to the prohibition mentioned in Section I shall be determined under the conditions provided for in Article 9(2) of Regulation (EU) 2016/679 of 27 April 2016 and in this Law.

[xxviii] **Article 3**

I. Without prejudice, with respect to processing falling within the scope of Regulation (EU) 2016/679 of 27 April 2016, to the criteria provided for in Article 3 of this Regulation, all of the provisions of this Law shall apply to the processing of personal data carried out as part of the activities of an establishment of a data controller or a data processor on French territory, whether or not the processing takes place in France.

II. National rules adopted on the basis of the provisions of the same Regulation, and which refer to national law the task of adapting or supplementing the rights and obligations provided for by this Regulation, shall apply when the data subject resides in France, including when the data controller is not established in France. However, when one of the processing operations mentioned in Article 85(2) of the same Regulation is involved, the national rules mentioned in the first paragraph of Section II shall be those to which the data controller is subject, when it is established in the European Union.

[xxix] **Section 5: Processing of Personal Data for the Purposes of Journalism and Literary and Artistic Expression**

Article 80

By way of derogation, the provisions of Article 4(5), those of Articles 6, 46, 48, 49, 50, 53, 118, 119 and those of Chapter V of Regulation (EU) 2016/679 of 27 April 2016 shall not apply, when such derogation is necessary to reconcile the right to protection of personal data and freedom of expression and information, to processing carried out for the purposes of :

1° Academic, artistic or literary expression;

2° Working as a journalist in a professional capacity, in compliance with the ethical rules of this profession. The provisions of the preceding paragraphs shall not preclude the application of the provisions of the French Civil Code, the laws relating to the written or audiovisual press and the French Criminal Code, which lay down the conditions for exercising the right of reply and which prevent, limit, remedy and, where appropriate, punish infringements of the privacy and reputation of persons.

[xxx] **Section 4: Processing for Archiving Purposes in the Public Interest, for Scientific or Historical Research Purposes, or for Statistical Purposes**

Article 78

When processing of personal data is implemented by public archiving services for archiving purposes in the public interest in accordance with Article L. 211-2 of the French Heritage Code, the rights provided for in Articles 15, 16 and 18 to 21 of Regulation (EU) 2016/679 of 27 April 2016 shall not apply insofar as these rights render impossible or seriously hinder the achievement of these purposes. The appropriate conditions and safeguards provided for in Article 89 of the same Regulation shall be determined by the French Heritage Code and the other legislative and regulatory provisions applicable to public archives. They shall also be ensured by compliance with state-of-the-art standards relating to electronic archiving.

A decree of the Council of State, issued after a reasoned and published opinion from the CNIL (Commission Nationale de l'Informatique et des Libertés [National Commission for Information Technology and Liberties]), shall determine under what conditions and subject to what safeguards the rights provided for in Articles 15, 16, 18 and 21 of the same

Regulation may be waived in whole or in part, with respect to processing for scientific or historical research purposes, or for statistical purposes.

[xxxi] **Article 79**

Under the conditions of Article 14(5)(b) of Regulation (EU) 2016/679 of 27 April 2016, when personal data were initially collected for another purpose, the provisions of Article 14(1) to (4) shall not apply to processing for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, or to the reuse of such data for statistical purposes under the conditions of Article 7 bis of Law No. 51-711 of 7 June 1951 on the obligation, coordination and confidentiality relating to statistics.

[xxxii] **Section 3: Processing for Archiving Purposes in the Public Interest, for Scientific or Historical Research Purposes, or for Statistical Purposes**

Article 116

The derogations provided for in the second paragraph of Article 78 of the aforementioned Law of 6 January 1978 relating to processing for scientific or historical research purposes or for statistical purposes shall apply only in cases where the rights provided for in Articles 15, 16, 18 and 21 of the aforementioned Regulation (EU) 2016/679 of 27 April 2016 would be likely to render impossible or seriously hinder the achievement of the specific purposes, and where such derogations are necessary to achieve these purposes.

The data resulting from this processing stored by the data controller or its data processor can only be accessed or modified by authorised persons. Such persons shall comply with the rules of ethics applicable to their sectors of activity.

The authorisations granted by data controllers to such persons shall comply with the specific purposes of the preceding paragraph and the safeguards provided for in the following paragraph.

Such data shall not be disseminated without prior anonymisation unless the interest of third parties in such dissemination prevails over the interests or fundamental rights and freedoms of the data subject. For research results, this dissemination must be absolutely necessary for its presentation. The data disseminated must be adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed. The dissemination of personal data appearing in documents consulted pursuant to Article L. 213-3 of the French Heritage Code can only take place after authorisation from the archive administration, after agreement from the authority that issued the documents, and after receiving the opinion of the statistical confidentiality committee established by Article 6 bis of Law No. 51-711 of 7 June 1951 on the obligation, coordination and confidentiality relating to statistics with respect to data covered by confidentiality relating to statistics.

[xxxiii] French Decree of application for French Data Protection Law: French Decree of application, No. 2019-536, of 29 May 2019, for French Data Protection Act

German Law

[xxxiv]: Federal Data Protection Act (BDSG), available in English here: Federal Data Protection Act (gesetze-im-internet.de)
Interstate Media Treaty (MStV), available in English here: Interstate Media Treaty (die-medienanstalten.de)
Artistic Copyright Act (KUG), available in German here: Artistic Copyright Act (gesetze-im-internet.de)
Network Enforcement Act (NetzDG), available in German here: Network Enforcement Act (gesetze-im-internet.de)

[xxxv] **Section 27 BDSG**
Data processing for purposes of scientific or historical research and for statistical purposes
(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research purposes or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

[xxxvi] **Section 28 BDSG**
Data processing for archiving purposes in the public interest
(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if necessary for archiving purposes in the public interest. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

[xxxvii] **Section 27 BDSG**
Data processing for purposes of scientific or historical research and for statistical purposes
(4) The controller may publish personal data only if the data subject has provided consent or if doing so is indispensable for the presentation of research findings on contemporary events.

[xxxviii] **Article 23 MStV**
Data Protection in Relation to Journalistic and Editorial Purposes

(1) Insofar as the state broadcasting corporations forming the ARD, the ZDF, Deutschlandradio, commercial broadcasters or companies and ancillary companies of the press—as providers of telemedia—process personal data for journalistic purposes, the persons involved are prohibited from processing this personal data for other purposes (data confidentiality). These persons shall be bound to data confidentiality when commencing their duties. Data confidentiality shall continue even after the termination of their duties. Except Chapters I, VIII, X and XI of Regulation (EU) 2016/679, only point (f) of Article 5(1) in conjunction paragraph (2), together with Articles 24 and 32 of Regulation (EU) 2016/679 shall apply to data processing for journalistic purposes. Articles 82 and 83 of Regulation (EU) 2016/679 shall apply, subject to the provision that liability shall be limited to data confidentiality breaches in accordance with sentences 1 to 3 and inadequate measures in accordance with point (f) of Articles 5(1), 24 and 32 of Regulation (EU) 2016/679. Chapter VIII of Regulation (EU) 2016/679 does not apply insofar as companies, ancillary companies and associated undertakings of the press are subject to self-regulation by the Press Code and the Complaints Procedure of the German Press Council. Sentences 1 to 6 shall apply accordingly to the ancillary companies and associated undertakings which are part of the bodies mentioned in sentence 1. The data subjects shall only be entitled to the rights outlined in paragraphs 2 and 3.

(2) In the event that personal data is stored, changed, transmitted, blocked or deleted for journalistic purposes by a provider of telemedia and this causes prejudice to the personal rights of the data subject, he or she may request information concerning his or her stored data. The information may be refused after the interests of the participants with legitimate grounds for protection are considered, provided that:
1. the data can be used to identify persons who have participated in the preparation, production, or distribution of the data;
2. the data can be used to infer the identity of the sender or the guarantor of contributions, documents, and communications for the editorial unit; or
3. the communication of the researched or otherwise gathered data could impair the journalistic task of researching the information repository.
The data subject may request the immediate rectification of inaccurate personal data in the data records or the addition of an adequate amount of data to better represent him or her. The continued storage of personal data is lawful when this is necessary for the exercise of the right to freedom of expression and information or for the safeguarding of legitimate interests. Sentences 1 to 3 shall not apply to offers by companies, ancillary companies and participating of the press insofar these are subject to self-regulation by the Press Code and the Complaints Procedure of the German Press Council.

(3) In the event that the processing of personal data for journalistic purposes leads to the dissemination of counterstatements of the data subject or to declarations of commitment, decisions or judgments on the omission of the

distribution or on the revocation of the content of the data, these counterstatements, declarations of commitment and revocations shall hence be included in the stored data and stored there for the same duration as the data itself and transmitted together with the data.

[xxxix] **Section 22 KUG**

Images may only be distributed or publicly displayed with the consent of the person portrayed. In case of doubt, consent shall be deemed to have been granted if the person depicted received remuneration for having his or her likeness reproduced. After the death of the person depicted, the consent of the relatives of the person depicted is required for a period of 10 years. Relatives within the meaning of this law are the surviving spouse or partner and the children of the person depicted and, if there is neither a spouse or partner nor children, the parents of the person depicted.

[xl] **Section 23 KUG**

(1) Without the consent required under Section 22, the following may be disseminated and displayed:
1. portraits from the field of contemporary history;
2. pictures in which the persons appear only as an accessory next to a landscape or other location;
3. pictures of meetings, processions and similar events in which the persons depicted took part;
4.portraits that are not made to order, provided that the dissemination or display serves a higher interest of art.

(2) However, the authorization shall not extend to dissemination and display that violates a legitimate interest of the person depicted or, if the person is deceased, of his or her relatives.

[xli] **Section 22 BDSG**

Processing of special categories of personal data

(2) …Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:
1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;
2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
3. measures to increase awareness of staff involved in processing operations;
4. designation of a data protection officer;
5. restrictions on access to personal data within the controller and by processors;
6. the pseudonymization of personal data;

7. the encryption of personal data;
8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
9. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

[xlii] **Section 27 BDSG**

Data processing for purposes of scientific or historical research and for statistical purposes

(1) …The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

…

(3) In addition to the measures listed in Section 22 (2), special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 processed for scientific or historical research purposes or statistical purposes shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject. Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research or statistical purpose.

[xliii] **Section 28 BDSG**

Data processing for archiving purposes in the public interest

(1) …The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

[xliv] **Section 27 BDSG**

Data processing for purposes of scientific or historical research and for statistical purposes

(2) The rights of data subjects provided in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes. Further, the right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the data are necessary for purposes of scientific research and the provision of information would involve disproportionate effort.

[xlv] **Section 28 BDSG**

Data processing for archiving purposes in the public interest

(2) The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the archival material is not identified with the person's name or no information is given which would enable the archival material to be found with reasonable administrative effort.

(3) The right of the data subject to rectification according to Article 16 of Regulation (EU) 2016/679 shall not apply if the personal data are processed for archiving purposes in the public interest. If the data subject disputes the accuracy of the personal data, he or she shall have the opportunity to present his or her version. The responsible archive shall be obligated to add this version to the files.

(4) The rights provided in Article 18 (1) (a), (b) and (d) and in Articles 20 and 21 of Regulation (EU) 2016/679 shall not apply as far as these rights are likely to render impossible or seriously impair the achievement of the archiving purposes in the public interest, and the exceptions are necessary to fulfil those purposes.

[xlvi] **Section 2 NetzDG**

Reporting obligation

(1) Social network providers who receive more than 100 complaints about unlawful content in a calendar year shall be obliged to prepare a German-language report on the handling of complaints about unlawful content on their platforms containing the information pursuant to subsection (2) every six months and to publish it in the Federal Gazette and on their own homepage no later than one month after the end of a half year. The report published on its own homepage must be easily recognisable, immediately accessible and permanently available.

(2) The report shall at least address the following aspects:
...
2. the nature, main features of operation and scope of any procedures used for the automated detection of content to be removed or blocked, including general information on training data used and on the provider's verification of the results of these procedures, as well as information on the extent to which scientific and research circles are supported in the evaluation of these procedures and have been granted access to the provider's information for this purpose,
...
13. information on whether and to what extent scientific and research circles were granted access to information from the provider during the reporting period to enable them to evaluate it anonymously, to what extent
a) removed or blocked unlawful content is linked to characteristics within the meaning of Section 1 of the General Equal Treatment Act of 14 August 2006 (Federal Law Gazette I p. 1897), as last amended by Article 8 of the Act of 3 April 2013 (Federal Law Gazette I p. 610), as amended,
(b) the dissemination of unlawful content leads to the specific concern of certain categories of users; and
(c) organised structures or concerted practices underlie the dissemination,
…

[xlvii] **Section 5a NetzDG**

Disclosure for scientific research

(1) A researcher within the meaning of this provision is any natural or legal person who conducts scientific research.

(2) A researcher may request qualified information from the provider of a social network about
1. the use and concrete mode of operation of procedures for the automated identification of content to be removed or blocked, in particular on the type and scope of technologies used and the purposes, criteria and parameters for their programming as well as on the data used,
2. the dissemination of content which has been the subject of complaints about illegal content or which has been removed or blocked by the provider, in particular the relevant content as well as information about which users have interacted with the content and in what way.

(3) Information pursuant to paragraph 2 may only be requested insofar as it is necessary for projects of scientific research in the public interest on the type, scope, causes and modes of action of public communication in social networks and the providers' handling thereof.

(4) Information may only be provided if the researcher presents a protection concept to the social network provider. The protection concept shall include
1. a description of the information required for the research purposes pursuant to paragraph 3,
2. a description of the intended use of the information,
3. a description of the precautions taken to prevent the information from being used for any other purpose,
4. a description of the arrangements to protect the provider's legitimate interests; and
5. a description of the technical and organisational measures that ensure the protection of personal data.

(5) The provider of a social network may refuse to provide information if
1. his or her interests worthy of protection significantly outweigh the public interest in the research, or
2. the interests of the persons concerned that are worthy of protection are impaired and the public interest in the research does not outweigh the confidentiality interests of the persons concerned.

(6) The provider of a social network may transmit the following personal data for the purpose of providing information pursuant to paragraph 2:
1. the disseminated content,
2. complaints about illegal content,
3. user names of those involved in the dissemination,
4. the detailed circumstances of the interactions of the participants in the dissemination with regard to the respective contents as well as
5. training data of procedures for the automated detection of content to be removed or blocked, as well as information on the mode of operation, purposes, criteria and parameters for programming these procedures.
The data shall be transmitted anonymously or at least pseudonymously, insofar as this is possible without jeopardising the purpose of the research.

(7) The researcher may process the data exclusively for the purposes of scientific research projects pursuant to paragraph 3. Insofar as special categories of data within the meaning of Article 9(1) of Regulation (EU) 2016/679 … (General Data Protection Regulation) …, as amended from time to time, are processed, the researcher shall provide appropriate and specific measures for this purpose to safeguard the interests of the data subject pursuant to Section 22(2), second sentence, of the Federal Data Protection Act. In addition to the measures mentioned there, the data must be anonymised within the meaning of Article 9(1) of Regulation (EU) 2016/679 as soon as this is possible according to the research purpose. Any further data protection requirements remain unaffected.

(8) The provider of a social network shall be entitled to reimbursement from the researcher of reasonable costs incurred in providing information pursuant to paragraph 2. In determining the reasonable amount, it shall be taken into account that the costs must not constitute a substantial obstacle to the exercise of the right to information. Section 287(1) of the Code of Civil Procedure shall apply mutatis mutandis. Subject to sentence 5, the recoverable costs may not exceed 5,000 euros. This amount may only be exceeded if the provision of the information results in exceptionally high costs. After submission of the protection concept in accordance with paragraph 4, the researcher may demand that the provider submit a cost estimate free of charge within a reasonable period of time.

[xlviii] Interstate Media Treaty

Irish Law

[xlix] **Irish Data Protection Act 2018** (as amended), available in English here: Data Protection Act 2018 (Irish Statute Book)

[l] **Section 54**

Irish Data Protection Act 2018 - Processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Subject to compliance with section 42 , the processing of special categories of personal data is lawful where such processing is necessary and proportionate for—

(a) archiving purposes in the public interest,

(b) scientific or historical research purposes, or

(c) statistical purposes.

[li] **Section 43**

Irish Data Protection Act 2018 - Data Processing and freedom of expression and information

43. (1) The processing of personal data for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression, shall be exempt from compliance with a provision of the Data Protection Regulation specified in subsection (2) where, having regard to the importance of the right of freedom of expression and information in a democratic society, compliance with the provision would be incompatible with such purposes.

(2) The provisions of the Data Protection Regulation specified for the purposes of subsection (1) are Chapter II (principles), other than Article 5(1)(f), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries and international organisations), Chapter VI (independent supervisory authorities) and Chapter VII (cooperation and consistency).

(3) The Commission may, on its own initiative, refer any question of law which involves consideration of whether processing of personal data is exempt in accordance with subsection (1) to the High Court for its determination.

(4) An appeal shall, by leave of the High Court, lie from a determination of that Court on a question of law under subsection (3) to the Court of Appeal.

(5) In order to take account of the importance of the right to freedom of expression and information in a democratic society that right shall be interpreted in a broad manner.

[lii] **Section 42**

Irish Data Protection Act 2018 - Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

(1) Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, personal data may be processed, in accordance with Article 89, for—

(a) archiving purposes in the public interest,

(b) scientific or historical research purposes, or

(c) statistical purposes.

(2) Processing of personal data for the purposes referred to in subsection (1) shall respect the principle of data minimisation.

(3) Where the purposes referred to in paragraph (a), (b) or (c) of subsection (1) can be fulfilled by processing which does not permit, or no longer permits, identification of data subjects, the processing of information for such purposes shall be fulfilled in that manner.

Section 36

Irish Data Protection Act 2018 - Suitable and specific measures for processing

(1) Where a requirement that suitable and specific measures be taken to safeguard the fundamental rights and freedoms of data subjects in processing personal data of those subjects is imposed by this Act or regulations made under this Act, those measures may include in particular the following—

(a) explicit consent of the data subject for the processing of his or her personal data for one or more specified purposes,

(b) limitations on access to the personal data undergoing processing within a workplace in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data,

(c) strict time limits for the erasure of personal data and mechanisms to ensure that such limits are observed,

(d) specific targeted training for those involved in processing operations, and

(e) having regard to the state of the art, the context, nature, scope and purposes of data processing and the likelihood of risk to, and the severity of any risk to, the rights and freedoms of data subjects—

(i) logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased,

(ii) in cases in which it is not mandatory under the Data Protection Regulation, designation of a data protection officer,

(iii) where the processing involves data relating to the health of a data subject, a requirement that the processing is undertaken by a person referred to in section 52(2) [Healthcare practitioner or a person with an equivalent duty of confidentiality],
(iv) pseudonymisation of the personal data, and
(v) encryption of the personal data.

[liii] **Section 61**
Irish Data Protection Act 2018 - Restriction on exercise of data subjects' rights: archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

(1) Subject to subsection (3), where processing of data is for archiving purposes in the public interest, the rights of a data subject set out in Articles 15, 16, 18, 19, 20 and 21 are restricted to the extent that—
(a) the exercise of any of those rights would be likely to render impossible, or seriously impair, the achievement of those purposes, and
(b) such restriction is necessary for the fulfilment of those purposes.
(2) Subject to subsection (4), where processing of data is for scientific or historical research purposes or statistical purposes, the rights of a data subject set out in Articles 15, 16, 18 and 21 are restricted to the extent that—
(a) the exercise of any of those rights would be likely to render impossible, or seriously impair, the achievement of those purposes, and
(b) such restriction is necessary for the fulfilment of those purposes.
(3) Where data is being processed for purposes referred to in subsection (1) and the processing serves another purpose at the same time, that subsection applies only to the extent that the processing relates to the purposes referred to in that subsection.
(4) Where data is being processed for purposes referred to in subsection (2) and the processing serves another purpose at the same time, that subsection applies only to the extent that the processing relates to the purposes referred to in that subsection.

Italian Law

[liv] **Italian Data Protection Code**, available in English here: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9740796

[lv] **Section 2-e**

Italian Data Protection Code - Processing of Special Categories of Personal Data That Is Necessary for Reasons of Substantial Public Interest

1. Processing of the special categories of data referred to in Article 9(1) of the Regulation that is necessary for reasons of substantial public interest in accordance with paragraph 2, letter g) thereof shall be allowed if it is provided for in EU law or, as regards the national legal system, in a law, a regulation, or an administrative instrument of a general nature; such law, regulation or administrative instrument of a general nature shall specify what types of data may be processed, what processing activities may be performed and what substantial public interest reasons justify the processing along with the suitable, specific measures to safeguard the data subject's fundamental rights and interests.

1-bis. Personal data relating to health shall be processed, after removing directly identifying information, by the Ministry of Health, the Istituto Superiore di Sanità [Higher Institute for Health], the National Agency for regional healthcare services, the Italian Medicine Agency, the National Institute for the promotion of health in migrant populations and for the fight against poverty-related diseases, and by Regions, with regard to the individuals using the respective services, also by way of the interlinking at national level of the individual information systems of the National Health Service including Electronic Health Records (FSE), which shall serve purposes compatible with those underpinning the processing at issue, in accordance with the purposes officially pursued by each of the aforementioned entities as well as with the arrangements and for the purposes set out in a decree by the Minister of Health, under the terms of paragraph 1 hereof, subject to an opinion given by the Garante, pursuant to the provisions made in the Regulation, this Code, the Digital Administration Code referred to in legislative decree No 82 of 7 March 2005, and the interoperability guidelines issued by the Agency for Digital Italy.

2. Without prejudice to paragraph 1, a substantial public interest shall be considered to exist in relation to processing activities performed by entities that carry out tasks in the public interest or in the exercise of official authority in the following sectors:

[…]

cc. Processing activities performed for archiving purposes in the public interest or for historical research purposes concerning preservation, cataloguing and communication of documents and records held in State archives, historical archives of public bodies, or private archives declared to be of especially substantial historical interest; processing activities for purposes of scientific research and processing for statistical purposes by entities belonging to the national statistics system (SISTAN);

[…].

3. As for genetic data, biometric data and data relating to health, processing shall be carried out in all cases pursuant to Section 2-f hereof.

[lvi] **Section 136**

Italian Data Protection Code - Journalistic Purposes and Other Intellectual Works

1. This Title shall apply in pursuance of Article 85 of the Regulation to processing operations

a) that are carried out in the exercise of the journalistic profession and for the sole purposes related thereto;

b) that are carried out by persons included either in the list of free-lance journalists or in the roll of trainee journalists as per Sections 26 and 33 of Law No 69 of 03.02.63; or

c) that are aimed exclusively at publishing or circulating, also occasionally, articles, essays and other intellectual works also in terms of academic, artistic or literary expression.

Section 137

Italian Data Protection Code - Applicable Provisions

1. With regard to the provisions made in Section 136, the data referred to in Articles 9 and 10 of the Regulation may be processed also without the data subject's consent providing the rules of conduct mentioned in Section 139 [Rules for journalistic activity] are abided by.

2. The processing activities referred to in Section 136 shall not be subject to the following:

a) The safeguards referred to in Section 2-f [Genetic, biometric or general health data], and Section 2p [high risk processing carried out in the public interest];

b) The provisions contained in Chapter V of the Regulation concerning transfers of personal data to third countries or international organisations.

3. If the data are communicated or disseminated for the purposes referred to in Section 136, the limitations imposed on freedom of the press to protect the rights as per Article 1(2) of the Regulation and Section 1 of this Code, in particular the essential nature of the information with regard to facts of public interest, shall be left unprejudiced. It shall be allowed to process the data concerning circumstances or events that have been made known either directly by the data subject or on account of the data subject's public conduct.

[lvii] **Section 101**

Italian Data Protection Code - Processing Arrangements

1. No personal data that has been collected for archiving purposes in the public interest or for historical research purposes may be used for taking measures or issuing provisions against the data subject in administrative matters, unless said data are also used for other purposes in compliance with Article 5 of the Regulation.

2. Any document containing personal data that is processed for archiving purposes in the public interest or for historical research purposes may only be used, by having regard to its nature, if it is relevant and indispensable for said purposes. Personal data that are disseminated may only be used for achieving the aforementioned purposes.

3. Personal data may be disseminated in any case if they relate to circumstances or events that have been made known either directly by the data subject or on account of the latter's public conduct.

Section 102

Italian Data Protection Code - Rules of Conduct Applying to Processing for Archiving Purposes in the Public Interest or for Historical Research Purposes

1. The Garante shall encourage adoption of rules of conduct in pursuance of Section 2-c by the private and public entities, including scientific societies and professional associations, that are involved in processing data for archiving purposes in the public interest or historical research purposes.

2. The rules of conduct referred to in paragraph 1 shall set out appropriate safeguards for the rights and freedoms of the data subject, and in particular:

a) rules based on fairness and non-discrimination in respect of users, to be abided by also in communication and dissemination of data, pursuant to the provisions of this Code and the Regulation that are applicable to the processing of data for journalistic purposes or else for publication of papers, essays and other intellectual works also in terms of artistic expression;

b) the specific safeguards applying to collection, access to and dissemination of documents concerning data disclosing health, sex life or confidential family-related matters; the cases shall be also specified where either the data subject or an interested party must be informed by the user of the planned dissemination; and

c) arrangements to apply the provisions on processing of data for archiving purposes in the public interest or historical research purposes to private archives, as also related to harmonisation of access criteria and the precautions to be taken in respect of communication and dissemination.

[lviii] **Section 110-a**

Italian Data Protection Code – Further processing of personal data by third parties for scientific research or statistical purposes

1. The Garante may authorise further processing of personal data, including the special categories of personal data referred to in Article 9 of the Regulation, for scientific research purposes or statistical purposes by third parties that carry out such activities to a prevailing extent if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes. In such cases, the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects in accordance with Article 89 of the Regulation including arrangements for the prior minimization and anonymization of the data.

2. The Garante shall communicate the decision adopted on the authorisation request within forty-five days; failing such communication, the request shall be considered to be rejected. When issuing the authorisation or thereafter following checks performed as appropriate, the Garante shall lay down the necessary conditions and measures to ensure adequate safeguards to protect data subjects in connection with the further processing of their personal data by third parties as also related to security issues.

3. Further processing of personal data by third parties for the purposes referred to in this Section may also be authorised by the Garante through decisions of general application to be adopted of its own motion as also related to specific categories of processing and controller. Those decisions shall set out the conditions for further processing and the necessary measures to ensure adequate safeguards to protect data subjects. The decisions adopted pursuant to this paragraph shall be published in the Official Journal of the Italian Republic. [The Garante has not yet implemented any general decisions under this paragraph]
4. Processing for scientific purposes of the personal data collected in the course of clinical activities by public and private *Istituti di ricovero e cura a carattere scientifico* shall not be an instance of further processing by third parties on account of the instrumental nature of the health care activities carried out by such *Istituti* vis-à-vis research activities, subject to compliance with Article 89 of the Regulation.

[lix] **Section 99**

Italian Data Protection Code - Duration of Processing

1. Processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may be carried out also for longer than is necessary for achieving the individual purposes for which the data had been previously collected or processed.
3. Where the processing of personal data is terminated, for whatever reason, such data may be kept or transferred to another data controller for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in compliance with Article 89(1) of the Regulation.

Section 100

Italian Data Protection Code - Data Concerning Studies and Researches

1. In order to encourage and support research and co-operation in the scientific and technological sectors, public bodies including universities and research institutions are empowered to decide that data concerning studies and researches, graduates, post-graduates, technicians and engineers, researchers, professors, experts and scholars be communicated and disseminated also to private bodies and by electronic networks – except for the data referred to in Articles 9 and 10 of the Regulation.
2. The data subject's rights of rectification, erasure, restriction and objection in pursuance of Articles 16, 17, 18 and 21 of the Regulation shall be left unprejudiced.
3. The data referred to in this Section shall not be regarded as administrative records under the terms of Law No 241 of 7 August 1990.
4. The data referred to in this Section may be processed further exclusively for the purposes for which they have been communicated or disseminated.

4-a. The rights referred to in paragraph 2 shall be exercised in accordance with the arrangements set out in the rules of conduct.

[lx] **Section 7**

Italian Data Protection Code - Exercise of rights

1. The archivist shall facilitate the exercise of the right of the persons concerned to rectify or supplement their data, ensuring that they are stored in a way that distinguishes the original sources from the documentation acquired subsequently.
2. For the purposes of applying Article 15 of the GDPR, in the event of a generalised request for access to a wide range of data or documents, the Archivist shall make available the relevant search tools and sources and provide the requester with suitable instructions for easy consultation.
3. In case of exercise of a right, concerning deceased persons pursuant to art. 2-terdecies of the Code, by a person who has his/her own interest or is acting on behalf of the data subject, in relation to personal data concerning deceased persons and very old documents, the existence of the interest shall also be assessed with reference to the time elapsed.

Luxembourgish Law

[lxi] **Luxembourg Data Protection Act** 2018, available in English here: Data Protection Act 2018 (cnpd.public.lu)

[lxiii] **Article 62**

Processing of personal data carried out for the sole purpose of journalism or academic, artistic or literary expression is not subject:
1° a) to the prohibition on processing special categories of data set out in Article 9, paragraph 1, of Regulation (EU) 2016/679;
b) to the limitations on processing of judicial data set out in Article 10 of Regulation (EU) 2016/679; when the processing relates to data manifestly made public by the data subject or to data in direct relation to the public life of the data subject or with the events in which they were voluntarily involved;
2° to Chapter V relating to transfers to third countries or international organisations of Regulation (EU) 2016/679; A 686 - 11
3° to the obligation to provide information according to Article 13 of Regulation (EU) 2016/679, where the application thereof would compromise the collection of data from the data subject;

4° to the obligation to provide information according to Article 14 of Regulation (EU) 2016/679, where the application thereof would compromise the collection of data, a planned publication, the making available, in any manner, of the data to the public , or would provide indications enabling the identification of the sources of information;
5° to the right of access of the data subject, which is deferred and limited in that it cannot concern information on the origin of the data, and/or enable the identification of a source of information. Subject to this limitation, access must be exercised via the intermediary of the CNPD in the presence of the president of the Press Council or their representative, or when the president of the Press Council has been duly summoned.

[lxiv] **Article 65**
Luxembourg Data Protection Act

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller of processing carried out for scientific or historical research purposes or statistical purposes, must implement the following additional appropriate measures:
1° the appointment of a data protection officer;
2° the performance of an impact assessment of the planned processing activities on the protection of personal data;
3° the anonymisation and pseudonymisation as defined in Article 4, paragraph 5 of Regulation (EU) 2016/679, or other operational separation measures guaranteeing that the data collected for scientific or historical research purposes or statistical purposes, cannot be used to adopt decisions or take actions concerning data subjects;
4° the use of a trusted third party, operationally independent from the controller, for the anonymisation or pseudonymisation of the data;
5° the encryption of personal data in transit and at rest, as well as state of the art key management;
6° the use of technology reinforcing the protection of the private lives of data subjects;
7° the use of access restrictions to personal data within the controller;
8° the use of a log file enabling the reason, date and time that data is consulted and the identity of the person collecting, modifying or deleting personal data to be retraced;
9° promoting the awareness of the staff involved about the processing of personal data and professional secrecy;
10° the regular evaluation of the effectiveness of the technical and organisational measures implemented through an independent audit;
11° the prior drawing up of a data management plan;
12° the adoption of the sector specific codes of conduct as set out in Article 40 of Regulation (EU) 2016/679, approved by the European Commission pursuant to Article 40, paragraph 9 of Regulation (EU) 2016/679. For each project for scientific or historical research purposes or statistical purposes, the controller must document and justify any exclusion of one or several of the measures listed in this article

[lxv] **Article 63**

Luxembourg Data Protection Act

Where personal data are processed for scientific or historical research purposes or for statistical purposes, the controller may derogate from the rights of the data subject as laid out in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679, insofar as these rights are likely to render impossible or seriously impair the achievement of specific purposes, subject to the implementation of appropriate measures as referred to in Article 65.

[lxv] **Article 64**

Luxembourg Data Protection Act

The processing of special categories of personal data as defined in Article 9, paragraph 1 of Regulation (EU) 2016/679, may be carried out for the purposes referred to in Article 9 paragraph 2, point j) of this same regulation, if the controller meets the requirements set out in Article 65.

Netherlands

[lxvi] **Dutch Implementing Act GDPR**, available in English here (informal translation): UAVG_ENG.pdf (hendriks-james.nl)

[lxvii] **Section 24**

Dutch Implementing Act - Exceptions for scientific or historical research or statistical purposes

Having regard to Article 9(2)(j) of the Regulation, the prohibition on processing special categories of personal data does not apply if:

a. processing is necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation;

b. the research referred to in a. serves a public interest;

c. it is impossible or would involve a disproportionate effort to request express consent; and

d. safeguards have been put in place for the processing such that the data subject's privacy is not disproportionately compromised.

[lxviii] **Section 43**

Dutch Implementing Act - Exceptions for journalistic purposes or purposes of academic, artistic or literary expression

1. This Act, with the exception of Sections 1 to 4 and 5(1) and (2), does not apply to the processing of personal data solely for journalistic purposes and for purposes solely of academic, artistic or literary expression.
2. The following chapters and articles of the Regulation do not apply to the processing of personal data solely for journalistic purposes and for purposes of academic, artistic or literary expression:
a. Article 7(3) and Article 11(2);
b. Chapter III;
c. Chapter IV, with the exception of Articles 24, 25, 28, 29 and 32;
d. Chapter V;
e. Chapter VI; and
f. Chapter VII.
3. Articles 9 and 10 of the Regulation do not apply in so far as the processing of the data referred to in those articles is necessary for journalistic purposes or for purposes of academic, artistic or literary expression.

[lxix] **Section 45**

Dutch Implementing Act

1. Articles 15, 16, 18(1)(a) and 20 of the Regulation do not apply to the processing of personal data that are part of records as referred to in Section 1(c) of the Public Records Act 1995 that are kept in a repository as referred to in Section 1(f) of that Act.
2. The data subject may obtain access to the records, unless requests for access are so vague that they cannot reasonably be granted.
3. If personal data are inaccurate, the data subject may add his or her own words to the records concerned

Spanish Law

[lxx] Organic Law 3/2018, of 5 December 2018, on the Protection of Personal Data and Guarantee of Digital Rights, available in Spanish here: https://www.boe.es/eli/es/lo/2018/12/05/3/con

[lxxi] ***Article 85. Right to rectification in the Internet***

1. Everyone has the right to freedom of expression on the Internet.

2. Those responsible for social networks and equivalent services shall adopt appropriate protocols to enable the exercise of the right of rectification by users who disseminate content that violates the right to honour, personal and family privacy on the Internet and the right to freely communicate or receive truthful information, in accordance with the requirements and procedures provided for in Organic Law 2/1984 of 26 March, regulating the right of rectification.

When the digital media must respond to a request for rectification formulated against them, they must proceed to publish in their digital archives a clarifying notice stating that the original news item does not reflect the current situation of the individual. This notice should appear in a prominent place alongside the original information.

[lxxii] The Constitutional Court has established a general rule that "the right of expression shall prevail in those cases in which the information published is, on the one hand, truthful, and on the other hand is of public relevance, being of general interest the matters and persons to which it refers". While jurisprudence has established this test, as there is no legislative framework, it is therefore necessary to carry out an "ad hoc" balancing exercise based on the principle of proportionality.