

Article

Experiences Regarding Anonymising and Publishing Personal Data as Open Data in Germany: Results of an Online Survey

Norbert Lichtenauer ^{1,*} , Lukas Schmidbauer ¹ , Florian Wahl ²  and Sebastian Wilhelm ² 

¹ Faculty of Applied Health Sciences, Deggendorf Institute of Technology, Health Campus Bad Kötzing, Landshuter Straße 1e, 93444 Bad Kötzing, Germany; lukas.schmidbauer@th-deg.de

² Faculty of Applied Computer Science, Deggendorf Institute of Technology, Technology Campus Grafenau, Hauptstraße 3, 94481 Grafenau, Germany; florian.wahl@th-deg.de (F.W.); sebastian.wilhelm@th-deg.de (S.W.)

* Correspondence: norbert.lichtenauer@th-deg.de; Tel.: +49-0991-3615-8392

Abstract

Introduction: The anonymisation of Personal Data (PD) and its release as Open Data (OD) hold considerable potential for innovation across health, research, public administration, and the economy. However, practical experiences regarding data anonymisation and OD publication remain underexplored in Germany. This study empirically investigates the current state of anonymised data practices, the barriers to implementation, and the desired support mechanisms for publishing formerly PD as OD. **Methods:** Embedded in a mixed-methods approach, this cross-sectional study examines research interest in the collection, processing, and use of anonymised data, as well as potential barriers and support services for the anonymisation and publication of former PD. A nationwide online survey was conducted in October–November 2024 via LimeSurvey. A total of 215 responses were included in the descriptive analysis. **Results:** The findings indicate limited experience with PD anonymisation and OD publication across industries. The potential added value of these processes was often not fully recognised, and data-handling responsibilities were rarely standardised. Data collectors, data protection officers, and IT departments were identified as the most frequently involved parties in these processes. Technical and educational support were the most desired forms of assistance. **Discussion:** To foster broader OD utilisation, stakeholders require comprehensive support. According to the sample, specific training and further education on the anonymisation and publishing process, as well as the desired software, are most important. Developing standardised process descriptions that integrate ethical and legal considerations, supported by national networks or governmental institutions, could significantly enhance the responsible and effective use of anonymised OD in Germany.

Keywords: open data; anonymisation; personal data; key persons; data use; data value creation



Academic Editors: Chingnung Yang and Mingxing Duan

Received: 1 October 2025

Revised: 8 December 2025

Accepted: 10 December 2025

Published: 17 December 2025

Citation: Lichtenauer, N.; Schmidbauer, L.; Wahl, F.; Wilhelm, S. Experiences Regarding Anonymising and Publishing Personal Data as Open Data in Germany: Results of an Online Survey. *Information* **2025**, *16*, 1111. <https://doi.org/10.3390/info16121111>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The further use of Personal Data (PD) after anonymisation as Open Data (OD) is widely discussed across industries and sectors. In business, public administration, research, and healthcare, comprehensive data analysis is considered an essential prospect for the future, generating added value for all stakeholders and improving overall quality of life [1]. For several years, numerous global efforts have been underway to develop further applications for OD [2,3]. A scoping review conducted in preparation for this study included 52 publications that described barriers and enabling factors for the further use

of OD. It became evident that the fields of business, government, research, and healthcare face broadly similar obstacles and supporting factors [1].

In the business sector, there is a broad consensus that the use of OD and big data plays a forward-looking role in innovation and service improvement [1]. The positive effects of OD use on economic growth have already been identified [4]. Consequently, the further use and processing of OD are regarded as key economic drivers [2,5]. At the same time, interviews have revealed limited knowledge and experience regarding the anonymisation of PD and its publication as OD. Therefore, staff capacity and expertise must be further developed [6]. Companies have expressed the need for governmental support, particularly in regard to providing OD platforms and establishing networks. Moreover, a secure legal framework for corporate use is not yet universally available [1]. The business sector has also called for practical tools to support data collection and analysis [2,6].

In the public sector, the increased use of anonymised government data, known as Open Governance Data (OGD), is described as having transformative value for society as a whole [4,5,7]. There are global efforts to establish OGD ecosystems, as significant cultural and institutional benefits are expected through improved services and innovations [4,7,8]. Although public authorities already publish large amounts of data, there remains considerable potential for further use and analysis [1,7]. At the same time, interviews have revealed numerous personnel-related, technical, and institutional challenges in implementing anonymisation processes and subsequent publication [6].

Similarly, in the field of research and the open science movement, there are calls for unrestricted access to scientific publications and raw research data [9] to reduce barriers to research results and to promote wide dissemination within the scientific community [6,10]. In 2018, the International Committee of Medical Journal Editors (ICMJE) issued recommendations for data sharing. However, recent studies have shown that substantial discrepancies remain between stated intentions and actual data accessibility [9]. The European Open Science Cloud (EOSC) strategy promotes data exchange and further analysis of publicly funded research [10]. Open science and the associated data analyses are expected to generate significant added value [11]. Furthermore, data collection resources must be used as efficiently as possible, taking ethical considerations into account, and repeated data collection should be avoided [1,12]. The cited scoping review also highlighted expected positive effects from collaboration and data standardisation, for example, through the FAIR principles (Findable, Accessible, Interoperable, and Reusable) [1].

Parallel to these developments, extensive added value is also expected from large-scale OD analyses in the healthcare sector [1,13]. The use of big data and OD in healthcare could, for example, enable more accurate prognoses or novel preventive diagnostic approaches, thereby improving treatment and efficiency [14–16]. The application of Artificial Intelligence (AI) and machine learning techniques in particular can reveal patterns and structures in data that significantly enhance diagnosis and treatment [17]. A scoping review revealed a lack of awareness regarding the potential of OD analyses in healthcare, as well as insufficient institutional support and inadequate technical tools [1].

Under the term Open Health Data (OHD), the European Union has been promoting increased use of health data since 2019 [18]. The European Health Data Space (EHDS) aims to enable cross-border data exchange of electronic health services [16,19]. However, patients and healthcare organisations continue to face numerous legal and ethical obstacles that hinder access to patient data [11]. As a result, a large portion of health data remains inaccessible, often locked in data silos [20].

Rapid technological developments have also raised new ethical and legal challenges in the analysis and use of OD [21–23], which in turn create additional practical barriers to the reuse of PD [24]. There are calls to establish comprehensive regulatory frameworks that

ensure data protection while maximising societal benefit [19,25]. Expert interviews have revealed considerable uncertainty across sectors about whether all legal requirements can be fully met, particularly regarding transparent consent procedures, data trusteeship, and ownership of raw data [6]. The European General Data Protection Regulation (GDPR) has set global standards for the collection and processing of PD [26]. The legal requirements of the GDPR have since been supplemented by the EU Data Governance Act (DGA) and the EU AI Act. The DGA, for example, aims to promote data altruism across Europe [26].

Regarding ethical aspects, expert interviews have primarily emphasised the need to regulate access to OD to foster acceptance and trust. Moreover, OD was understood as a purpose-driven use serving the public good rather than purely commercial objectives [6]. An international scoping review also found that there are currently few technical tools supporting anonymisation and publication processes that integrate legal and technical standards while ensuring user trust and security. At the same time, the targeted development and application of such practical software tools were explicitly demanded across sectors [1].

Interviews on experiences regarding the anonymisation, use, and reuse of PD as OD in Germany revealed primarily personnel-related, technical, and institutional challenges. Economic barriers were identified in the costs associated with anonymisation and publication, as well as concerns about innovation protection and increased competitive pressure related to OD provision. Technical barriers included inadequate infrastructure and significant heterogeneity of collected PD. Personnel-related obstacles were most frequently mentioned, such as a lack of interest from management or insufficient trust in technology [6]. In particular, limited knowledge and experience with anonymisation and the publication of PD were highlighted as key challenges [6]. At the same time, there are hardly any extensive empirical surveys in Germany on existing institutional experiences with anonymisation and publication of PD.

The *EAsyAnon* project at the Deggendorf Institute of Technology (DIT), funded by the German Federal Ministry of Research, Technology and Space (BMFTR), addresses these needs by developing a practical, automated software system to support the anonymisation of PD. A recommendation system analyses locally processed datasets in compliance with data protection regulations and proposes legally compliant anonymisation concepts tailored to specific requirements [27]. Following external anonymisation, the *EAsyAnon* system evaluates the quality of the process through a semi-automated audit [28]. To ensure that the system is closely aligned with user experience, the present study specifically investigated previous experiences with anonymisation and data publication across Germany and across sectors. The empirical research was therefore designed to capture explicit experiences with anonymisation and prior publication practices, and to conduct a nationwide survey of the current state of knowledge to improve the usability and practicality of the *EAsyAnon* software system under development.

2. Methods

Taking the above background into account, a quantitative online questionnaire survey was conducted across Germany to obtain detailed insights into the current level of experience with the anonymisation of PD and its subsequent publication as OD, and to incorporate specific support requirements into the development process.

2.1. Research Questions and Objectives

This study addressed the following research questions to healthcare institutions, research organisations, public authorities, and companies in Germany:

1. How are PD primarily collected and utilised within the respective domains?
2. What institutional experience exists regarding the anonymisation of PD and their publication as OD?
3. What barriers are encountered in everyday practice?
4. What types of support services are considered most helpful in anonymising collected PD and publishing them as OD?
5. What specific legal and ethical implications have been identified for the processes of anonymisation and publication, based on previous practical experience?

2.2. Research Design

Parallel to the technical development of *EAsyAnon*, empirical research was conducted to address the above research questions and to integrate prior experiences, needs, and articulated support requirements from the relevant domains into the development process. A mixed-methods approach was selected, combining qualitative and quantitative research designs [29,30], which is well-suited to the research subject. Findings were derived from a triangulation of methods: a systematic literature analysis in the form of a scoping review [1], a qualitative interview study to identify key aspects [6], and a subsequent large-scale quantitative questionnaire survey presented here (Figure 1). This approach enables a comprehensive investigation of the research topic by integrating multiple methodological perspectives. Within this mixed-methods framework, an exploratory sequential design was employed, in which the two sub-studies were conducted consecutively, with the findings of the first informing the subsequent surveys [31].

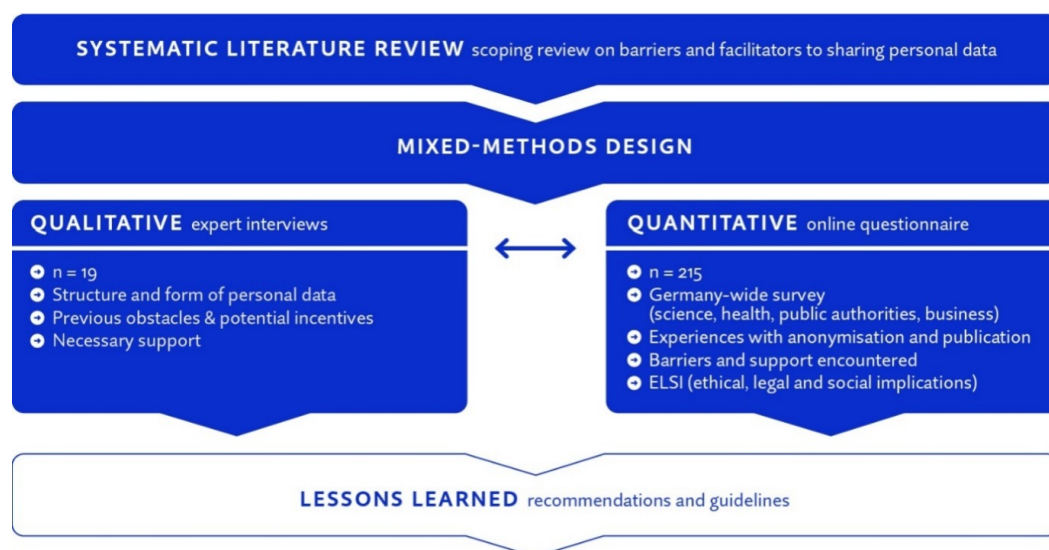


Figure 1. Overview of the empirical research within the *EAsyAnon* project. The empirical work comprised three sub-studies: (1) a scoping review [1], (2) qualitative expert interviews [6], and (3) a quantitative online survey. The sequential mixed-methods design ensured that earlier findings informed subsequent data collection and analysis.

2.3. Quantitative Method

An online survey was selected as the quantitative sub-study format. The questionnaire was developed based on previous findings from the literature review [1] and interviews analysis [6], and will be provided as Supplementary Materials to this article. The development followed a recognised scientific framework for constructing question catalogues [32]. In total, the questionnaire comprised ten categories with 116 items addressing experiences with anonymisation and publication, preferred support services, perceived barriers, and legal and ethical implications. A cognitive pretest was conducted to identify lin-

guistic and content-related issues concerning comprehensibility, relevance, and potential redundancies [33]. For this purpose, the completed questionnaire was first presented internally to the entire research team, who provided feedback using a standardised form. Following iterative revisions, three additional pretests were conducted with external participants, during which various metacognitive assessment strategies, such as paraphrasing and think-aloud protocols, were applied.

2.4. Sample

The sample was recruited by automatically collecting functional email addresses listed in the website's legal notices related to data protection. Using an in-house Python 3.7 script, 40,644 email addresses were collected from the websites of universities, research institutions, public authorities, hospitals, and companies across all 16 federal states in Germany. Publicly available lists and compilations were used to ensure that the sample was as broad and diverse as possible. A detailed description of the crawling procedure is provided as Supplementary Materials to this article.

2.5. Data Collection

The questionnaire was distributed to 40,644 email addresses throughout Germany using the online tool *LimeSurvey*, which was self-hosted within the university's IT infrastructure. Access permissions were limited to the directly involved researchers. The entire procedure was reviewed and approved by the university's DPO! (DPO!) and recorded in the official register of processing activities in accordance with Art. 30 GDPR. Invitations were sent via *LimeSurvey* from a neutral university email address (noreply@th-deg.de), accompanied by a standardised cover letter, which is provided in the Supplementary Materials. Following the initial invitation email, which included information about the research project, recipients were given the option to opt out of the distribution list if they did not wish to participate in the survey ($n = 102$). In addition, recipients were encouraged to forward the invitation to relevant experts with appropriate experience, either within their institution or externally, using the snowball sampling principle. The email explicitly stated that responses would be collected anonymously via *LimeSurvey*.

The invitation was also disseminated through the research group's professional networks, and regular posts were published on *LinkedIn*.

After four weeks, the response rate was very low, at 3.44 % ($n = 140$). Consequently, a reminder email was sent via *LimeSurvey* to the sample, and the survey period was extended by an additional four weeks (the text used for the reminder email is provided as Supplementary Materials). At the same time, social media activity on *LinkedIn* was intensified, and the research group's network was informed again.

In total, the survey phase lasted 52 days (25 September 2024 to 15 November 2024) and yielded 215 completed questionnaires, corresponding to a response rate of 5.29 per mille. The low response rate and the use of a snowball sampling method suggest a considerable potential for bias, which is discussed in detail in the limitations section of the article.

After the online survey was completed, all imported email addresses were immediately deleted from *LimeSurvey*. Furthermore, in compliance with applicable legal and research ethics standards, the crawled email addresses were permanently deleted following data collection.

All raw data, as well as the SPSS (Version 29.01.0) syntax file, are available as open data free of charge via Zenodo (DOI: <https://doi.org/10.5281/zenodo.17571648>).

2.6. Inclusion and Exclusion Criteria

At the beginning of the questionnaire, the first page provided comprehensive information about the *EAsyAnon* project and included an informed consent statement [34], which

participants were required to read and accept before proceeding. Participants were given sufficient time to consider their decision and could discontinue the questionnaire at any point without consequences. Filter questions were then applied to ensure compliance with the inclusion criteria (Table 1). If the criteria were not met, the questionnaire was automatically terminated.

Table 1. Inclusion criteria for participation in the nationwide online survey.

Inclusion Criteria
• Age of majority • Capacity to provide informed consent • Sufficient knowledge of German to complete the questionnaire • Relevant experience in the field of OD and anonymisation, in particular as data protection officers or other domain experts • Organisational role related to OD, anonymisation, or data processing/data protection/data management (e.g., DPO, ISB, data administration) komm

2.7. Ethics & Data Protection

To proactively and consistently address ethical and data protection considerations in the research project [35], an application was submitted to the Joint Ethics Commission of Bavarian Universities (GEHBa) prior to the empirical studies accompanying *EAsyAnon*. The application was approved (No. GEHBa-202309-V-124). All data protection aspects of the quantitative data collection were documented in a dedicated data protection concept, which was submitted to the Ethics Committee in compliance with legal requirements and in accordance with the principles of good scientific practice.

2.8. Data Analysis and Quality Criteria

The questionnaire was accessed 2287 times; however, only fully completed questionnaires were included in the analysis ($n = 215$). Owing to the small number of participants in specific subgroups, particularly within the health and research sectors, a purely descriptive analysis was conducted. This approach aimed to avoid response bias and misinterpretation of results for specific subgroups.

The descriptive analysis was performed using SPSS (Version 29.01.0) and Excel (Version 2511). After initial data processing in Excel, the cleaned dataset was imported into SPSS. Only fully completed questionnaires were included in the analysis ($n = 215$). For many categories and questions, however, the sample size varied due to missing values or questionnaire filtering. Respondents who did not answer a specific question were excluded from the analysis of that subquestion; thus, the sample sizes differ across items. Furthermore, recommendations from the EQUATOR Network (Enhancing the Quality and Transparency of Health Research) for reporting quantitative studies were followed. In the present study, the Checklist for Reporting of Survey Studies for Quantitative Methodology (CROSS) [36] was observed and is available as Supplementary Materials to this article.

All values were rounded to two decimal places, which may result in minor rounding errors. Consequently, totals in figures or tables may not always add up to exactly 100%.

3. Results

For specific questions, differing sample sizes (n) are reported in the analysis. Some categories and items were not displayed due to missing responses, filter routing, or participants' lack of experience with the processes. Following the sociodemographic description of the sample, the questionnaire categories are presented descriptively in relation to the research questions outlined above.

3.1. Sociodemographic Data

A total of 215 questionnaires were included in the evaluation. The average age of the respondents was 50.2 years and the median age was 52 years (range 22–78 years). The respondents who provided information about their sex ($n = 207$), showed a significantly higher proportion of men at 71.98% ($n = 149$) according to women with 26.57% ($n = 55$) and 1.45% ($n = 3$) identified as diverse. Among the respondents who indicated the sector they work in ($n = 211$), most assigned themselves to the private sector (46.45%; $n = 98$), followed by public institutions (45.97%; $n = 97$), non-profit organisations (4.74%; $n = 10$), and other sectors (2.84%; $n = 6$). Regarding the professional role of respondents ($n = 211$) (Figure 2), the most frequently cited position was data protection officer (46.45%; $n = 98$), followed by owner/management with 23.70% ($n = 50$), executives with 12.32% ($n = 26$), employees with 11.37% ($n = 24$) and other roles with 6.16% ($n = 13$). The category ‘Other’ included activities in organisation/digitalisation, IT manager, IT department, data protection manager, information security and data protection officer, research data management, quality management coordinator, municipal manager, data protection coordinator, and digitalisation and information security officer.

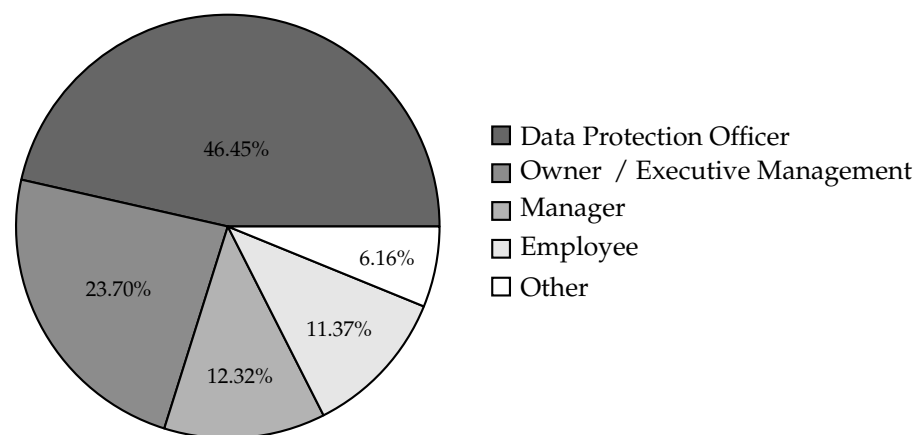


Figure 2. Roles of respondents in their institutions or companies ($n = 211$). Percentages indicate the share of respondents selecting each role: data protection officers (46.45%, $n = 98$), executive management (23.70%, $n = 50$), managers (12.32%, $n = 26$), employees (11.37%, $n = 24$), and other roles (6.16%, $n = 13$).

Respondents who provided information about the size of their institution or company ($n = 211$, Figure 3) most frequently reported working in large companies with more than 251 employees (30.33%; $n = 64$). They were followed by micro-enterprises with up to 10 employees (28.44%; $n = 60$) and institutions and companies with 51 to 250 employees (21.80%; $n = 46$). Institutions and companies with 11 to 50 employees participated least in the survey with 19.43% ($n = 41$).

The largest proportion of respondents identified themselves as working in public administration ($n = 78$) followed by companies and institutions focusing on consulting ($n = 37$) and research & development and services ($n = 17$ each). Other sectors included crafts/construction ($n = 16$), information technology ($n = 16$), health ($n = 11$), industry ($n = 9$), energy ($n = 1$), and transport ($n = 1$). The category ‘Other’ ($n = 10$) included church institutions, welfare organisations, the advertising industry, electronics development, nature conservation, social welfare providers, media, and research and consulting. Two respondents ($n = 2$) did not provide any information about the sector in which they work. This resulted in a highly heterogeneous sample with a focus on individuals from the public administration sector.

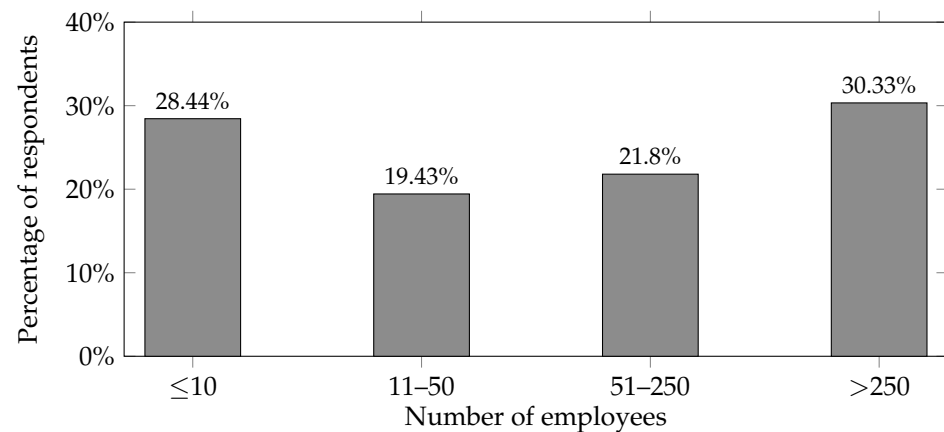


Figure 3. Size of institutions and companies by number of employees ($n = 211$). Among the respondents, 30.33% ($n = 64$) were affiliated with large organisations (>250 employees), 28.44% ($n = 60$) with micro-enterprises (≤ 10 employees), 19.43% ($n = 41$) with small enterprises (11–50 employees), and 21.80% ($n = 46$) with medium-sized enterprises (51–250 employees).

3.2. Categorical Evaluation

The **first research question** investigated how PD was collected, processed, and stored by the involved sectors in Germany following the provisions of the GDPR. A total of $n = 212$ respondents provided information on data collection. 82.08% ($n = 174$) of the PD collected was obtained using a combination of handwritten and electronic forms. In only 15.04% of the sample, PD was collected purely electronically ($n = 34$) and in 0.47% ($n = 1$) exclusively by hand. Regarding data processing, responses from $n = 211$ participants were available. Synonymous with collection, 69.67% ($n = 147$) of respondents also indicated a mixture of electronic and analogue processing in the further processing of PD. Only 28.91% ($n = 61$) were processed electronically alone; no cases of exclusively manual further processing were reported. For data storage, $n = 210$ valid responses were available. In 66.19% of cases ($n = 139$), the data were most frequently stored both on paper and electronically. A proportion of 32.86% ($n = 69$) was stored exclusively electronically, and 0.48% ($n = 1$) was stored purely on paper. In the case of long-term data archiving, $n = 209$ respondents answered this question, while three did not provide information. Similarly, long-term data archiving showed that 67.46% ($n = 141$) were archived both on paper and electronically, a further 30.62% ($n = 64$) were archived exclusively electronically, and 0.48% ($n = 1$) was archived on paper.

In addition, the sample was asked how many different individuals had PD available (Figure 4). In the sample of valid responses ($n = 214$), 29.91% ($n = 64$) most frequently reported 501 to 5000 PD in the institution/company. A further 23.83% ($n = 51$) stated that they had stored between 5001 and 50,000 PDs, 19.16% ($n = 41$) indicated that they had stored more than 50,000 PDs, and 22.43% ($n = 48$) said that they had fewer than 500 PDs. This means that 72.90% of the sample reported having at least 500 PD, and more than 42.99% reported having more than 5000 PD in their institution/company.

In addition, respondents were asked about their use of the collected PD. Suppose the responses are combined into a dichotomy (agreement = ‘agree’ and ‘tend to agree’; disagreement = ‘tend to disagree’ and ‘disagree’), 94.84% ($n = 202$) of the respondents use the internal PD exclusively for the originally specified purpose. In total, $n = 213$ responses were received, with two ($n = 2$) respondents indicating “don’t know”. Furthermore, 46.92% ($n = 99$) of respondents see potential added value in the existing PD for third parties, while 41.71% ($n = 88$) do not see this, and 11.37% ($n = 24$) stated “don’t know”. Here, a total of $n = 211$ responses were included. In addition, a minority (33.02%, $n = 70$) of respondents stated that the potential for internal use of existing PD is fully exploited, while

a majority (56.60%, $n = 120$) disagreed, and 10.38% ($n = 22$) stated “don’t know”. In total, $n = 212$ responses were analysed for this question. Furthermore, 22.65% ($n = 48$) of respondents said that anonymised PD has internal reuse, while 75.00% ($n = 158$) disagreed, and 2.36% ($n = 5$) stated “don’t know”. The total number of responses for this question was $n = 212$.

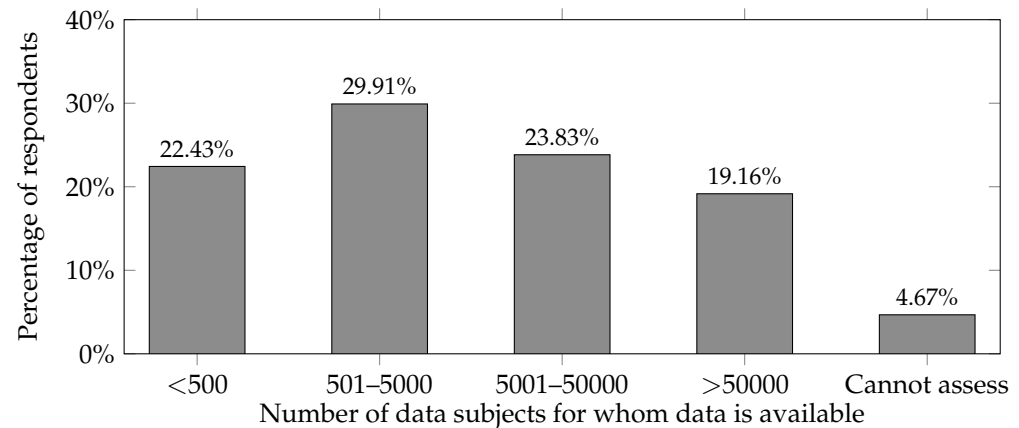


Figure 4. Number of data subjects with available PD per institution/company ($n = 214$). Overall, 72.90% ($n = 156$) reported at least 500 records, 42.99% ($n = 92$) reported more than 5000, and 19.16% ($n = 41$) more than 50,000 records.

Respondents were also asked whether and how the collected PD is already being shared ($n = 213$; Figure 5). Here, 59.15% ($n = 126$) of respondents stated that there is an obligation to share PD with third parties, while 36.62% ($n = 78$) had no responsibility, and 4.23% ($n = 9$) were unaware of any obligation. In addition, 60.09% ($n = 126$) said that anonymised data is not made available to third parties, while 33.33% ($n = 71$) already do so, and 6.57% ($n = 14$) did not provide any information on this question. Furthermore, 33.33% ($n = 71$) stated that they also pass on PD to third parties in non-anonymised form, for example, based on contracts. In comparison, a majority of 59.15% ($n = 126$) said that they do not do so, and 7.51% ($n = 16$) did not provide any information on this.

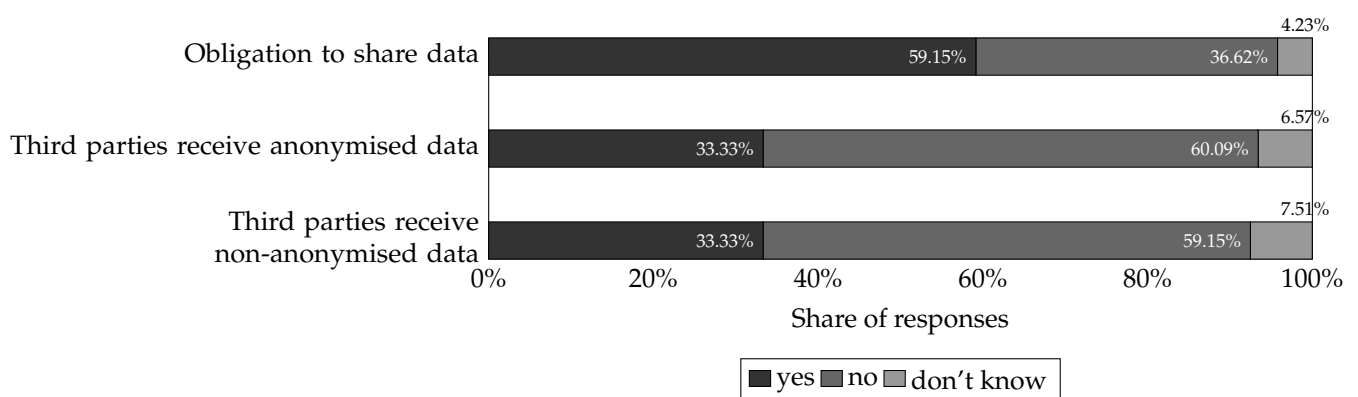


Figure 5. Disclosure of PD to third parties, anonymised and non-anonymised ($n = 213$). An obligation to share PD was reported by 59.15% ($n = 126$) of respondents; 33.33% ($n = 71$) already provide anonymised datasets externally, and 33.33% ($n = 71$) share non-anonymised PD under contractual arrangements.

The **second research question** surveyed the experiences of the sectors involved in anonymising the collected PD voluntarily and publishing it as OD.

Of the respondents ($n = 215$; Figure 6), 50.23% ($n = 108$). It stated that the institution/company already had experience with data anonymisation. A further 35.81%

($n = 77$) reported no experience whatsoever, and 13.95% ($n = 30$) did not know whether the institution/company had any experience with anonymisation.

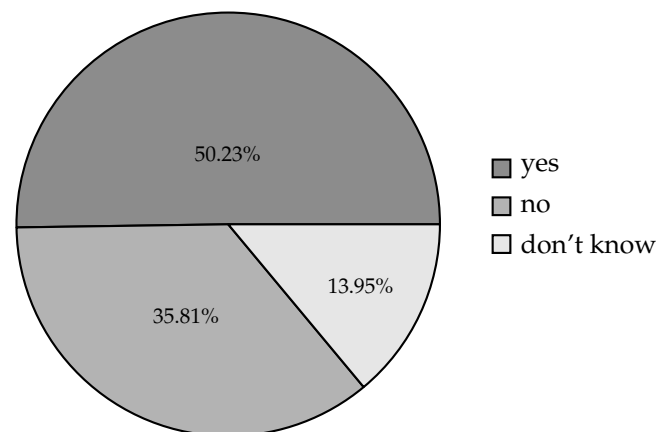


Figure 6. Institutional experience with anonymisation processes ($n = 215$). Half of all institutions (50.2%, $n = 108$) reported prior anonymisation experience; 35.81% $n = 77$ had none, and 13.95% $n = 30$ were uncertain.

The individuals who reported experience with anonymisation ($n = 81$; Table 2) were asked who was involved in the anonymisation process. It was found that the department where the PD was collected initially was most frequently involved in planning (30.86%, $n = 25$) the anonymisation process, followed by management positions (18.52%, $n = 15$) and IT security officers (11.11%, $n = 9$). In terms of implementing anonymisation, the data collector and specialist department were also most frequently responsible (50.62%, $n = 41$), followed by the IT department (38.27%, $n = 31$) and marketing (4.94%, $n = 4$). Data protection officers most frequently assumed a reviewing role (43.21%, $n = 35$), followed by IT security officers (23.46%, $n = 19$) and management (16.05%, $n = 13$). The IT department (23.46%, $n = 19$), data protection officers (19.75%, $n = 16$), and the legal department (14.81%, $n = 12$) provided the most support in the anonymisation process. The management (30.86%, $n = 25$), the IT security officer (13.58%, $n = 11$), and marketing and quality management (11.11% each $n = 9$) were mainly only informed.

Table 2. Involvement of different roles and departments in anonymisation processes ($n = 81$). Percentages represent the proportion of respondents indicating each level of involvement (planning, execution, review, etc.). Data-collecting departments executed anonymisation most frequently (50.62%, $n = 41$), followed by IT departments (38.27%, $n = 31$).

Involved Party	Planning	Executing	Reviewing	Supporting	Only Informed	Not Involved	Not Existing
Data Collecting Department	30.86%	50.62%	1.23%	9.88%	3.70%	1.23%	2.47%
IT Department	7.41%	38.27%	1.23%	23.46%	4.94%	16.05%	8.64%
Data Protection Officer	9.88%	2.47%	43.21%	19.75%	8.64%	9.88%	6.17%
Legal Department	1.23%	0.00%	11.11%	14.81%	9.88%	18.52%	44.44%
Compliance	3.70%	1.23%	6.17%	4.94%	7.41%	12.35%	64.20%
Marketing	3.70%	4.94%	1.23%	3.70%	11.11%	50.62%	24.69%
Management	18.52%	2.47%	16.05%	8.64%	30.86%	19.75%	3.70%
Quality Management	2.47%	3.70%	8.64%	7.41%	11.11%	12.35%	54.32%
IT Security Officer	11.11%	3.70%	23.46%	11.11%	13.58%	14.81%	22.22%

Furthermore, the respondents ($n = 81$; Figure 7) specified their experiences with anonymisation. 53.09% ($n = 43$) stated that anonymisation is carried out regularly, while 44.44% ($n = 36$) denied this and 2.47% ($n = 2$) did not provide any information. Fixed

responsibilities for one person in connection with anonymisation were indicated by 45.68% ($n = 37$), with a majority of 48.15% ($n = 39$) seeing no fixed responsibilities for this in the institution/company, and 6.17% ($n = 5$) not providing any information. A concrete process description for anonymisation was available for 33.33% ($n = 27$) of respondents, while 58.02% ($n = 47$) did not have such a description, and a further 8.64% ($n = 7$) of respondents were not aware of any such description.

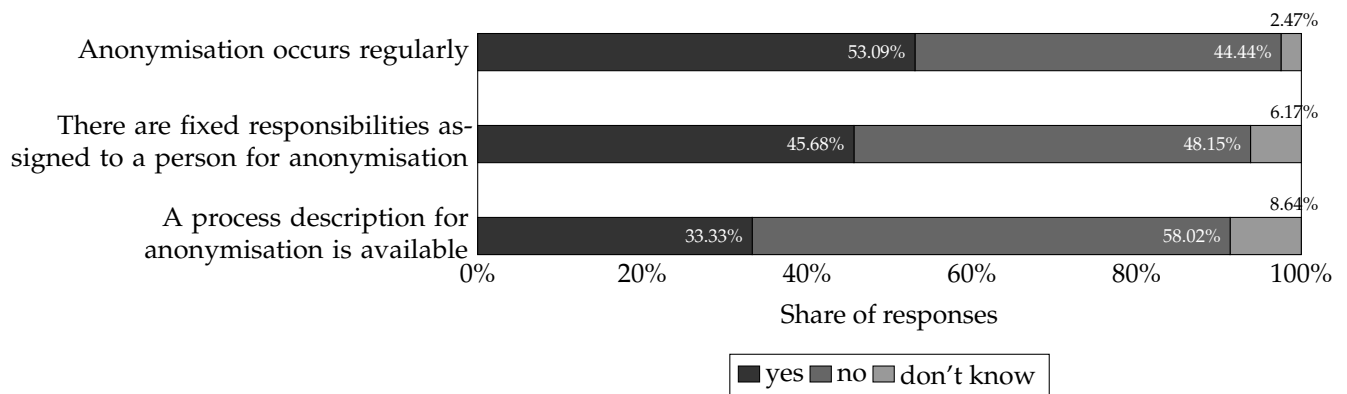


Figure 7. Organisational practices regarding anonymisation: regular occurrence, assigned responsibilities, and existence of process descriptions ($n = 81$). Regular anonymisation occurs in 53.09% ($n = 43$) of institutions; 45.68% ($n = 37$) have fixed responsibilities, and 33.33% ($n = 27$) maintain written process descriptions.

When asked which type of data anonymisation is most relevant in practice ($n = 215$; Figure 8), structured data was cited most frequently (77.67%, $n = 167$), followed by image files (35.35%, $n = 76$) and unstructured files (30.70%, $n = 66$). In contrast, the prevailing opinion was that anonymisation was not necessary for the majority of audio and video files. In an open question, semi-structured data (e.g., emails), data from electronic evaluations, data available as PDF files (e.g., wage evaluations, traffic measurements, visitor guidance), files in DICOM format from imaging diagnostics in the clinic, and telemetry data (e.g., personal tachographs) were specified as special data types for which anonymisation would be helpful.

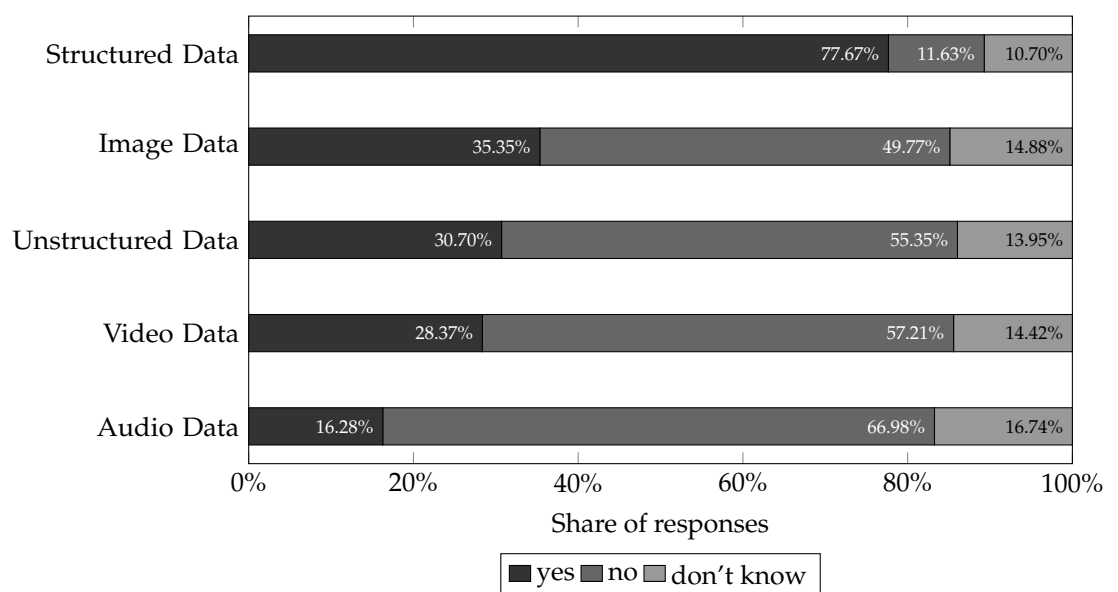


Figure 8. Types of data considered relevant for anonymisation ($n = 215$). Structured data (77.67%, $n = 167$) were considered most relevant, followed by image files (35.35% $n = 76$) and unstructured data (30.70%, $n = 66$).

Furthermore, respondents were asked about their existing expertise in the anonymisation process (Figure 9). When the response scale was dichotomised into agreement and disagreement, a majority of respondents indicated expertise in existing legal assessments (90.67%, $n = 68$ agreement among $n = 75$ respondents), followed by expertise in structured data (86.49%, $n = 64$ among $n = 74$ respondents), technical evaluation (84.72%, $n = 61$ among $n = 72$ respondents), and ethical evaluation (74.24%, $n = 49$ among $n = 66$ respondents) of anonymisation. Only a half of 50.00% ($n = 35$ among $n = 70$ respondents) reported expertise in unstructured data, and a minority of 40.0% ($n = 26$ among $n = 65$ respondents) reported expertise in the anonymisation of image files.

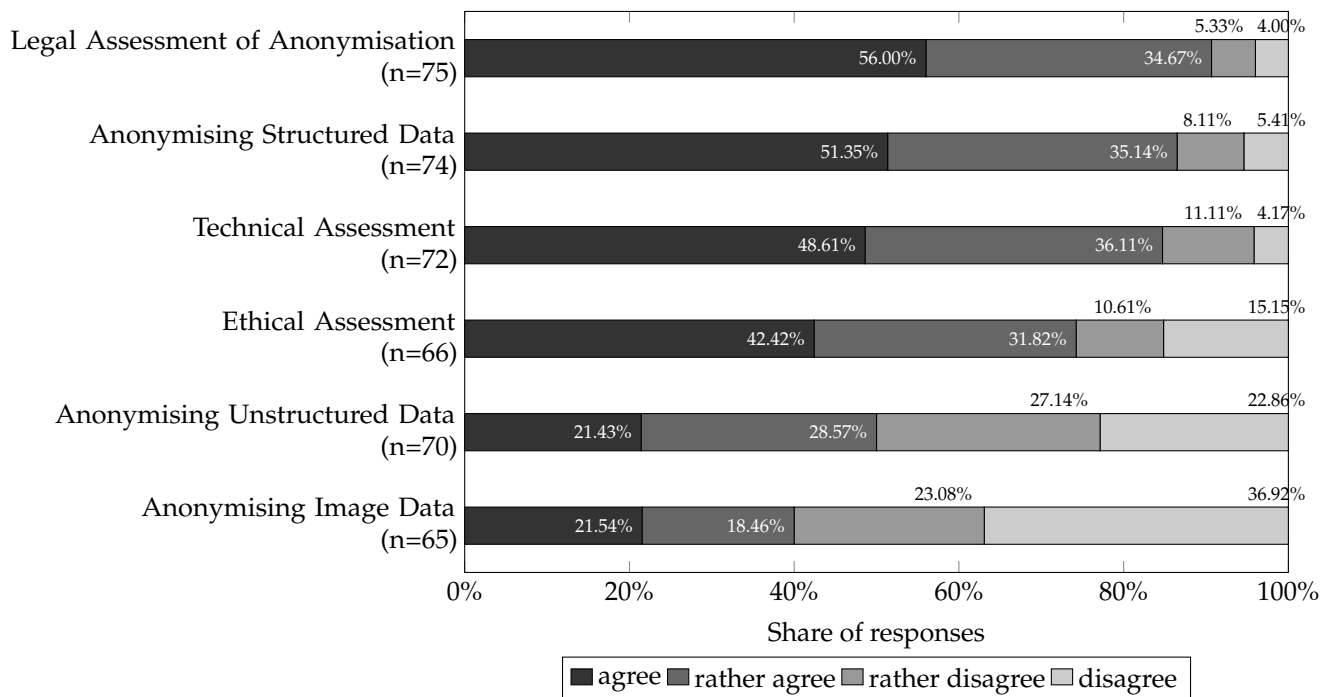


Figure 9. Existing expertise of respondents in different aspects of anonymisation. High expertise was reported for legal assessment (90.67%, $n = 68$ agreement among $n = 75$ respondents), structured data (86.49%, $n = 64$ among $n = 74$ respondents), and technical evaluation (84.72%, $n = 61$ among $n = 72$ respondents). Lower expertise was found for unstructured (50.0%, $n = 35$ among $n = 70$ respondents) and image data (40.0%, $n = 26$ among $n = 65$ respondents).

When asked about their experience in publishing anonymised PD all participants in the sample responded ($n = 215$). Only 30.23% ($n = 65$) stated that they already had experience with publication processes. In comparison, a clear majority of 58.61% ($n = 126$) had no experience whatsoever in publishing anonymised, formerly PD 11.16% ($n = 24$) were unable to answer the question. In addition, those with existing experience ($n = 45$) were asked whether the publications had been carried out due to external obligations or voluntarily. Data was published due to external commitments in 80.00% ($n = 36$) of cases, while this was not the case in 8.89% ($n = 4$) of cases, and was unknown in 11.11% ($n = 5$) of cases. Forty-four people answered the question regarding voluntary publication. Here, 70.45% ($n = 31$) had already voluntarily published anonymised data, while 15.91% ($n = 7$) said they had not, and 13.64% ($n = 6$) said they did not know whether voluntary publication had already taken place.

Furthermore, processes relating to publication were surveyed and multiple responses were possible here. ($n = 47$, Figure 10). About publication, 65.96% of respondents ($n = 31$) stated that they regularly publish anonymised data. In 57.45% ($n = 27$) of cases, fixed

responsibilities were specified for persons responsible for the publication of data. However, only 29.79% ($n = 14$) regulate the publication of data through a process description.

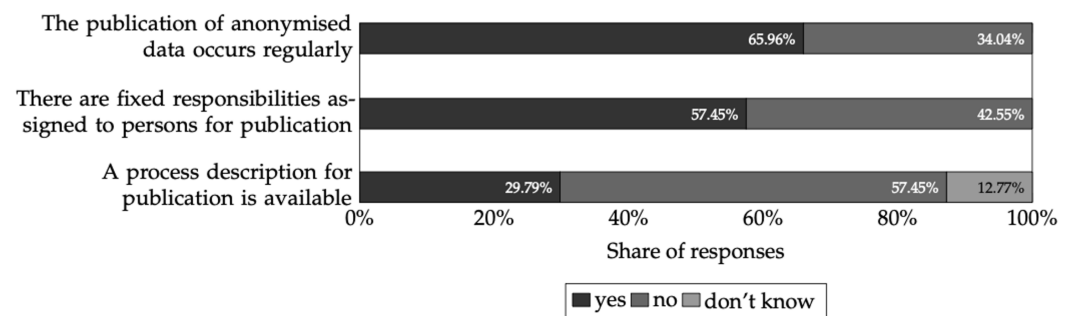


Figure 10. Organisational practices regarding the publication of anonymised data: frequency, responsibilities, and process descriptions ($n = 47$). Regular publication was confirmed by 65.96% ($n = 31$), fixed responsibilities by 57.45% ($n = 27$), but written process descriptions existed in only 29.79% ($n = 14$).

In parallel with the question regarding anonymisation, the individuals with experience ($n = 44$) were also asked which individuals were predominantly involved in the publication process (Table 3). Similar it was found that the department where the data was collected was most frequently involved in planning (25.00%, $n = 11$), followed by management positions (13.64%, $n = 6$) and the IT department (6.82%, $n = 3$). The original department was also most frequently responsible for executing the publication (54.55%, $n = 24$), followed by marketing (18.18%, $n = 8$) and management positions (13.64%, $n = 6$). As a rule, data protection officers took on a reviewing role (34.09%, $n = 15$), followed by IT security officers (22.73%, $n = 10$) and the legal department (20.46%, $n = 9$). The IT department (38.64%, $n = 17$), the legal department (4.55%, $n = 2$), and the department where the data was collected (11.36%, $n = 5$) were named as the most supportive. In most cases, only managers (40.91%, $n = 18$), data protection officers (18.18%, $n = 8$), and marketing (13.64%, $n = 6$) were informed about the publication. This meant that the department was most frequently involved in planning (25.00%, $n = 11$) and execution (54.55%, $n = 24$). In comparison, data protection officers were primarily involved in reviewing (34.09%, $n = 15$), and the IT department (38.64%, $n = 17$) was most frequently involved in providing support. Furthermore, managers were most frequently only informed (40.91%, $n = 18$). Marketing was not involved most frequently (31.82%, $n = 14$).

Table 3. Involvement of different roles and departments in publication processes ($n = 44$). Percentages represent the proportion of respondents indicating each level of involvement (planning, execution, review, etc.). Data-collecting departments most frequently executed the publication of anonymised data (54.48%, $n = 24$), followed by marketing (18.18%, $n = 8$) and management (13.64% $n = 6$).

Involved Party	Planning	Executing	Reviewing	Supporting	Only Informed	Not Involved	Not Existing
Data Collecting Department	25.00%	54.55%	2.27%	11.36%	2.27%	0.00%	4.55%
IT Department	6.82%	9.09%	4.55%	38.64%	2.27%	27.27%	11.36%
Data Protection Officer	6.82%	0.00%	34.09%	20.45%	18.18%	18.18%	2.27%
Legal Department	6.82%	0.00%	20.45%	4.55%	9.09%	25.00%	34.09%
Compliance	4.55%	2.27%	11.36%	0.00%	2.27%	9.09%	70.46%
Marketing	4.55%	18.18%	2.27%	9.09%	13.64%	31.82%	20.45%
Management	13.64%	13.64%	15.91%	2.27%	40.91%	13.64%	0.00%
Quality Management	4.55%	2.27%	13.64%	4.55%	4.55%	13.64%	56.82%
IT Security Officer	4.55%	4.55%	22.73%	9.09%	11.36%	27.27%	20.45%

Furthermore, individuals with experience of publication ($n = 55$, Table 4) provided information about their personal experiences. 14.55% ($n = 8$) stated that their experiences were very positive, while 29.09% ($n = 16$) had had rather positive experiences. A majority of 54.55% ($n = 30$) reported relatively neutral experiences, and only a very small proportion of 1.82% ($n = 1$) had rather negative experiences.

Table 4. Self-reported experiences with the publication of anonymised data ($n = 55$). Most respondents described their experience as neutral (54.54%, $n = 30$), 29.09% ($n = 16$) as rather positive, 14.54% ($n = 8$) as very positive, and 1.82% ($n = 1$) as rather negative.

	Frequency	Valid Percent
neutral	30	54.54%
very positive	8	14.54%
rather positive	16	29.09%
rather negative	1	1.82%
Total	55	100.0%

In addition, the individuals with experience of publication ($n = 55$) were asked where these datasets were published, with multiple answers possible (see Figure 11). The publication of anonymised data was most common on the organisation's website ($n = 28$), followed by government data portals ($n = 26$). Private sector data portals were mentioned less frequently ($n = 12$), as was the use of non-profit data portals ($n = 8$). In addition, publication was carried out jointly with the press, in reports to ministries, in scientific articles, in presentations, and doctoral theses and final theses.

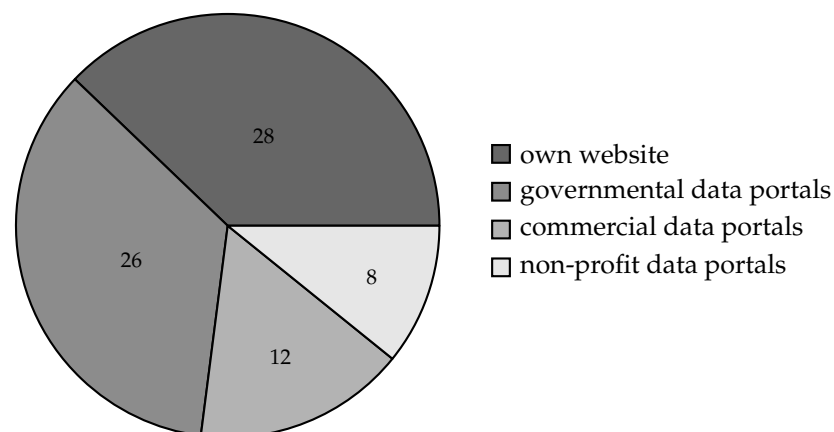


Figure 11. Publication venues of anonymised data ($n = 55$). Most respondents published data on their own websites or on governmental portals, while commercial and non-profit portals were less common.

Furthermore, respondents were asked about their **understanding of OD** ($n = 213$). 69.48% ($n = 148$) of respondents agreed with the statement that OD should only be provided with controllable access, while 16.43% ($n = 35$) disagreed and 14.08% ($n = 30$) did not answer. Similarly, 67.14% ($n = 143$) agreed with the statement that there should be clear restrictions on the use of OD, while only 15.96% ($n = 34$) disagreed and 16.90% ($n = 36$) did not respond. At the same time, a clear majority of 58.69% ($n = 125$) were in favour of providing OD free of charge, while 18.31% ($n = 39$) believed that it should not be free of charge, and 23.00% ($n = 49$) did not express a clear opinion on this. Similarly, a majority of 54.67% ($n = 117$) were in favour of OD containing anonymised data without exception, while 23.83% ($n = 51$) rejected this and 21.50% ($n = 46$) did not comment on this. At the same time, 27.57% ($n = 59$) were in favour of OD being possible even without anonymisation, while 44.39% ($n = 95$) rejected this, and 28.04% ($n = 60$) did not express a

clear opinion. When asked whether OD requires licensing, 46.48% ($n = 99$) believed that OD should generally be provided under a licence, while 25.35% ($n = 54$) rejected this and 28.17% ($n = 60$) did not give a clear answer.

Previous **experience with OD** was also surveyed ($n = 211$, Figure 12). The statement regarding intended future use of OD received the most agreement (42.18%, $n = 89$), with 18.48% ($n = 39$) rejecting future use and 39.34% ($n = 83$) not providing any information on this. A minority of 22.64% ($n = 48$) stated that they already use OD, while a clear majority of 59.43% ($n = 126$) said that they do not yet use OD, and a further 17.92% ($n = 38$) did not provide any information on this. The current existence of internal initiatives for the use of OD in institutions and companies was affirmed by 13.27% ($n = 28$), while 53.55% ($n = 113$) denied this, and 33.18% ($n = 70$) did not provide any information on this.

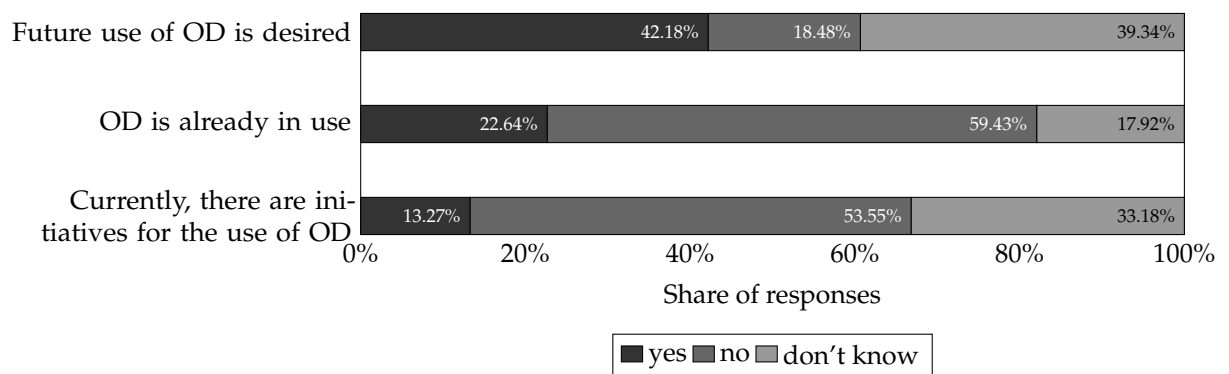


Figure 12. Experience with OD: current and future use, as well as internal initiatives ($n = 211$). OD is already used by 22.64% ($n = 48$) of respondents; 42.18% ($n = 89$) plan future use. Only 13.27% ($n = 28$) reported existing internal OD initiatives.

About the importance of OD ($n = 212$, Figure 13), only 13.21% ($n = 28$) of respondents in the sample considered the availability of OD to be essential, and 27.36% ($n = 58$) considered it to be important. Furthermore, 25.47% ($n = 54$) considered availability to be less critical, and 11.32% ($n = 24$) stated that OD was not important at all for the institution/company and 22.64% ($n = 48$) did not provide any information. If the answers are dichotomised, most respondents consider the availability of OD to be critical (40.57%; $n = 86$), while an almost equally large proportion consider the availability of OD to be less important or not necessary for the institution/company (36.59%, $n = 78$).

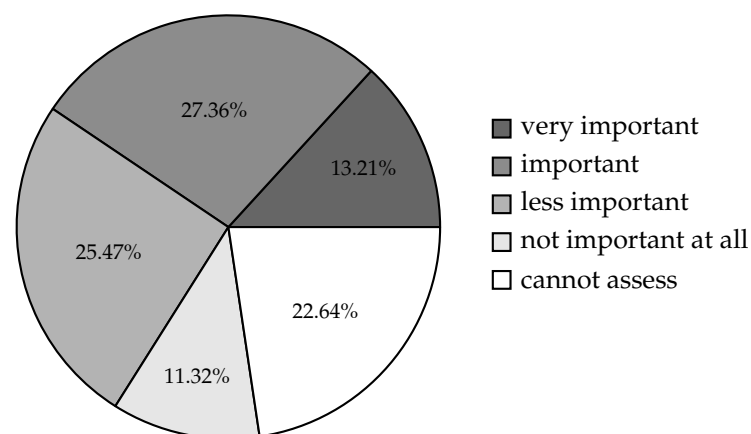


Figure 13. Perceived importance of OD for institutions and companies ($n = 212$). OD was considered very important by 13.21% ($n = 28$) and important by 27.36% ($n = 58$); 25.47% ($n = 54$) rated it less important and 11.32% ($n = 24$) not important at all.

Specific aspects relating to OD were also surveyed ($n = 212$, Figure 14). Regarding the statement that OD use is expected by management, only 5.19% ($n = 11$) of respondents agreed completely, while 13.21% ($n = 28$) agreed somewhat. In contrast, 23.58% ($n = 50$) somewhat disagreed and 40.09% ($n = 85$) disagreed with this statement, while 17.92% ($n = 38$) were unable to answer the question. When asked whether an internal OD policy already exists, 3.30% ($n = 7$) agreed and 3.77% ($n = 8$) somewhat agreed with the statement. A further 8.02% ($n = 17$) tended to disagree, and 64.62% ($n = 137$) disagreed, while 20.28% ($n = 43$) did not provide any information on this. When asked whether an OD culture is practised in the institution/company, only 1.89% ($n = 4$) agreed completely and 10.38% ($n = 22$) agreed somewhat. A majority of 56.13% ($n = 119$) disagreed, and 16.04% ($n = 34$) somewhat disagreed. No assessment was given by 15.57% ($n = 33$). If the statements are dichotomised into agreement and disagreement, the respondents stated that only 18.40% ($n = 39$) expect OD to be used by management. Only a small proportion (7.08%, $n = 15$) believed that an OD policy was already in place or progress, and a further 12.26% ($n = 26$) stated that an OD culture was actually practised in the institution/company. A large majority rejected the statements that OD use is expected by management (63.68%, $n = 135$), that an OD policy is already in place (72.64%, $n = 154$), and that an OD culture is practised (72.17%, $n = 153$).

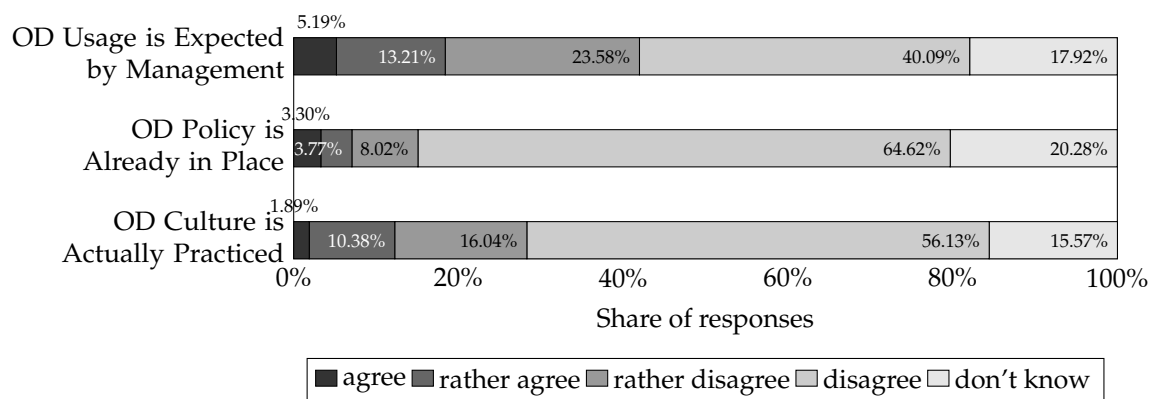


Figure 14. Internal aspects of OD: management expectations, existing policies, and OD culture ($n = 212$). OD use is expected by management in 18.40% ($n = 39$) of institutions, an OD policy exists in 7.08% ($n = 15$), and an OD culture is actively practised in 12.26% ($n = 26$).

The third research question investigated the barriers perceived by anonymising the PD they collect and subsequently publishing it as OD. Negative experiences in connection with OD were surveyed (Figure 15). The most frequently cited negative experience in connection with anonymisation processes was the very high time expenditure (34.62%, $n = 9$ among $n = 26$ respondents), followed by technical barriers (27.27%, $n = 6$ among $n = 22$ respondents) and personnel and institutional barriers, each at 25.00%, $n = 5$ among $n = 24$ respondents. This was followed by experiences relating to an unsuitable data structure (22.22%, $n = 4$ among $n = 18$ respondents), uncertainties about the possible misuse of data (20.83%, $n = 4$ among $n = 24$ respondents), and the threat of unfavourable competitive situations (9.09%, $n = 2$ among $n = 22$ respondents) resulting from the publication of data. When the responses regarding agreement and disagreement were dichotomised, the high time expenditure was most frequently cited as a negative experience (76.92% agreement, $n = 20$ among $n = 26$ respondents), followed by a lack of knowledge and personnel barriers (79.17% agreement, $n = 19$ among $n = 24$ respondents). Technical barriers led to negative experiences in 63.64% ($n = 14$ among $n = 22$ respondents) of cases. Furthermore, uncertainties about data misuse (45.83% $n = 11$ among $n = 24$ respondents), an unsuitable data structure (61.12%, $n = 11$ among $n = 28$ respondents), and institutional

barriers (45.83%, $n = 11$ among $n = 24$ respondents) were cited as negative experiences. Threatening competitive situations were the least responsible for negative experiences regarding the publication of OD, at 27.27% ($n = 6$ among $n = 22$ respondents). In an open question, further negative experiences were cited due to errors in anonymisation, a possible request from data subjects disclosure data, and the difficulty of finding suitable standards for anonymising data.

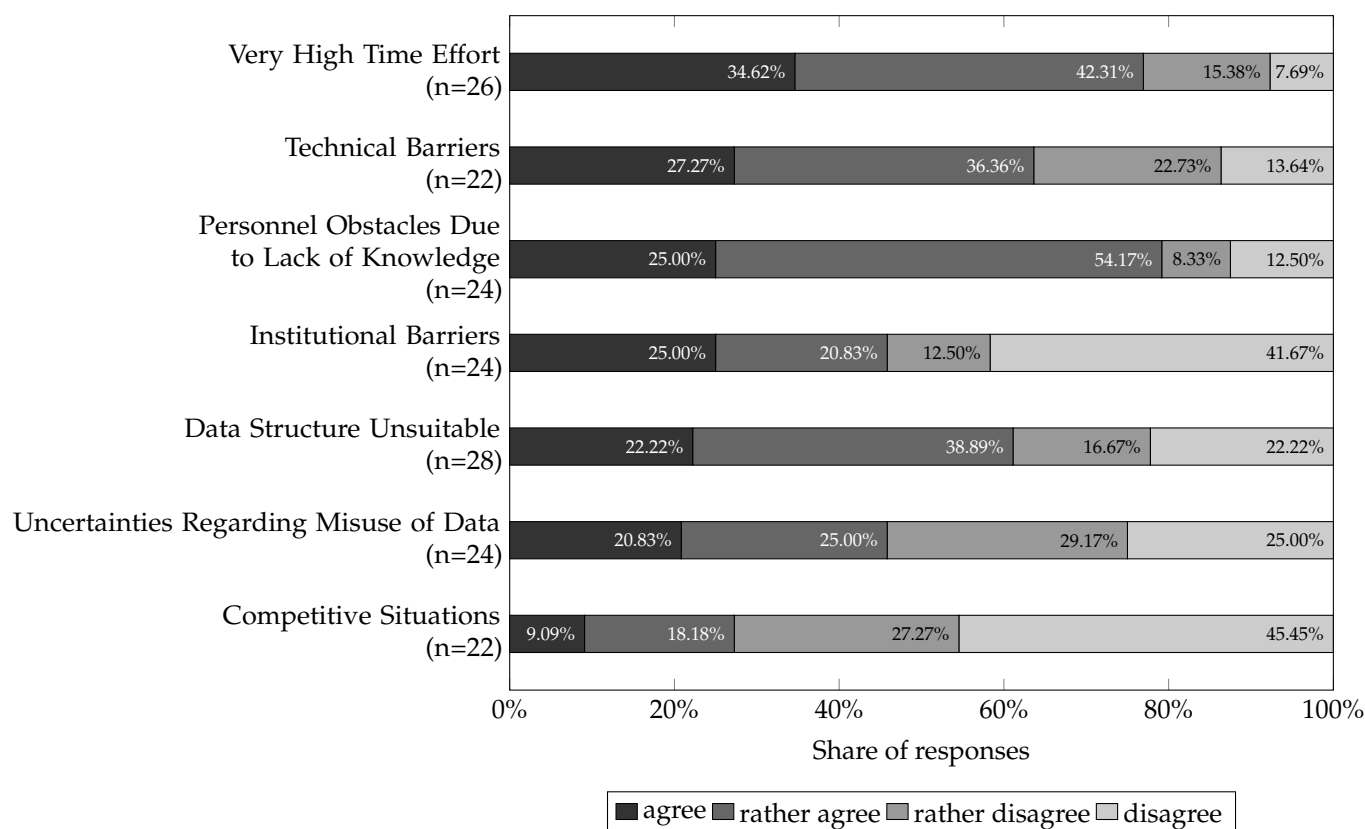


Figure 15. Negative experiences and barriers related to anonymisation and publication of OD. Main obstacles were high time effort (76.92%, $n = 20$ among $n = 26$ respondents), lack of knowledge (79.17%, $n = 19$ among $n = 24$ respondents), personnel shortages (79.17%, $n = 19$ among $n = 24$ respondents), and technical barriers (63.64%, $n = 14$ among $n = 22$ respondents). Concerns about data misuse (45.83%, $n = 11$ among $n = 24$ respondents) and unsuitable data structures (61.11%, $n = 11$ among $n = 18$ respondents) were also frequent.

The **fourth research question** addressed the necessary support services mentioned by the involved sectors to ensure that the collected PD is anonymised voluntarily and published as OD (Figure 16).

In the sample, software solutions (39.49%, $n = 77$ among $n = 195$ respondents) were most frequently considered to be very interesting support services. This was followed by training courses on anonymisation with 29.90% ($n = 61$ among $n = 204$ respondents) and general training courses on OD with 27.94% ($n = 57$ among $n = 204$ respondents). Other interesting options were support from authorities (26.46%, $n = 50$ among $n = 189$ respondents), recognised certification (24.86%, $n = 46$ among $n = 185$ respondents), and training on publication (19.40%, $n = 39$ among $n = 201$ respondents).

The **final research question** sought to identify specific legal and ethical aspects to anonymise the collected PD voluntarily and publish it as OD (Figure 17).

If the responses of the sample are dichotomised into agreement and disagreement regarding the legal implications of OD, the statement that the use of AI about OD can only be resolved through regulation (81.15%, $n = 155$ among $n = 191$ respondents) received

the highest level of agreement. This is followed by the importance of purpose limitation in the use of OD (71.88%, $n = 138$ among $n = 192$ respondents) and the need for a solid legal framework for OD concerning liability and anonymisation (87.01%, $n = 134$ among $n = 154$ respondents). In addition, a majority agreed that there are still many concerns about de-anonymisation (65.57%, $n = 120$ among $n = 183$ respondents), that there should be no obligation to obtain consent and provide information to data donors for anonymisation in OD (63.93%, $n = 117$ among $n = 183$ respondents), and that their own institution/company complies with all legal requirements for OD (74.17%, $n = 112$ among $n = 151$ respondents). A narrow majority also supported a state supervisory authority for OD (58.29%, $n = 109$ among $n = 187$ respondents). There was a dichotomy in the statement that liability for OD providers should be excluded (50.56%, $n = 91$, in favour and 49.44%, $n = 89$ among $n = 280$ respondents, against), as well as in the statement that the OD process is hampered by too many laws and regulations (52.57%, $n = 92$, in favour, 47.43%, $n = 83$ among $n = 175$ respondents, against). The majority rejected the idea that there should be a legal obligation to provide OD under certain conditions (62.16%, $n = 115$ among $n = 185$ respondents).

In addition, responses regarding ethical implications of OD were dichotomised (Figure 18). The majority of respondents agreed with the statements that the principle of data minimisation should be observed in OD (75.79%) and that there should be a principle of reciprocity in OD donations and OD benefits (62.01%). There was also a high level of agreement (72.12%) that Germany has more fears than other countries, as well as with the statement that access to OD must be regulated by an ethics committee (51.68%). The institutions/companies surveyed were relatively confident (71.69%) that they would comply with all ethical requirements in OD processes. The statements that ethical concerns hinder the anonymisation of PD (37.42%) and that an ethical discussion on the effects of OD is unnecessary (28.66%) were rejected by a majority.

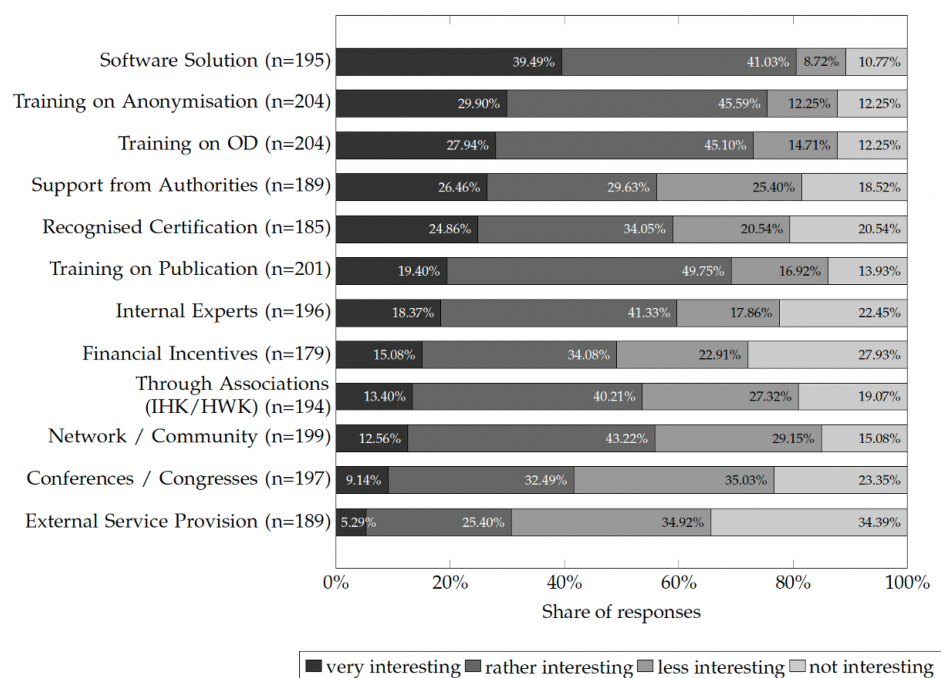


Figure 16. Preferred support services for anonymisation and publication of OD. Most respondents considered software solutions very interesting (39.49%, $n = 77$ among $n = 195$ respondents), followed by training on anonymisation (29.90%, $n = 61$ among $n = 204$ respondents), OD (27.94%, $n = 57$ among $n = 204$ respondents), and support from authorities (26.46%, $n = 50$ among $n = 189$ respondents).

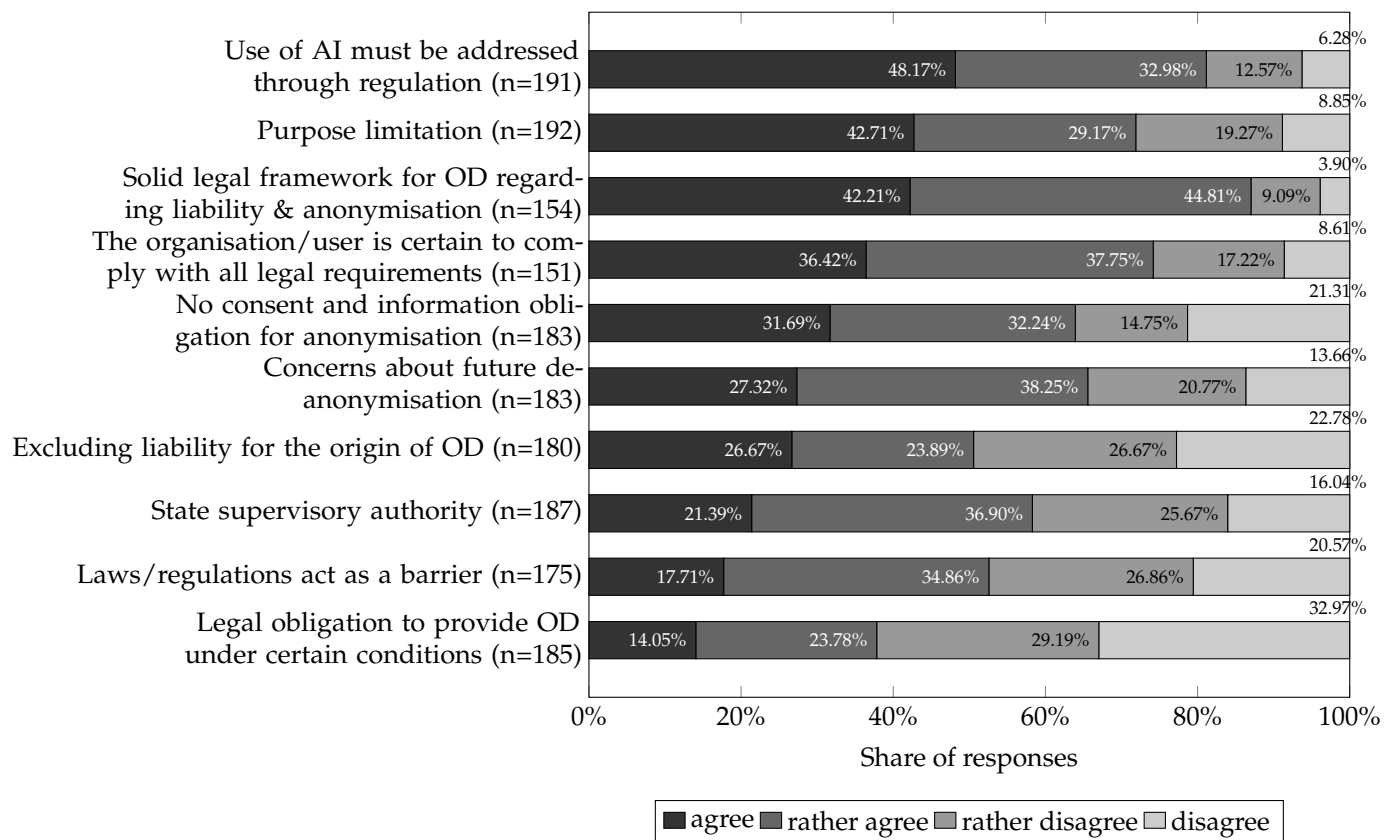


Figure 17. Perceived legal implications of OD, including regulation, liability, and de-anonymisation concerns. Agreement was highest for the need for a solid legal framework (87.01%, $n = 134$ among $n = 154$ respondents), AI-specific regulation (81.15%, $n = 155$ among $n = 191$ respondents), and concern about possible de-anonymisation (65.57%, $n = 120$ among $n = 183$ respondents). About 58.29% ($n = 109$ among $n = 187$ respondents) favoured a state supervisory authority, while 62.16% ($n = 115$ among $n = 185$ respondents) opposed a legal duty to provide OD.

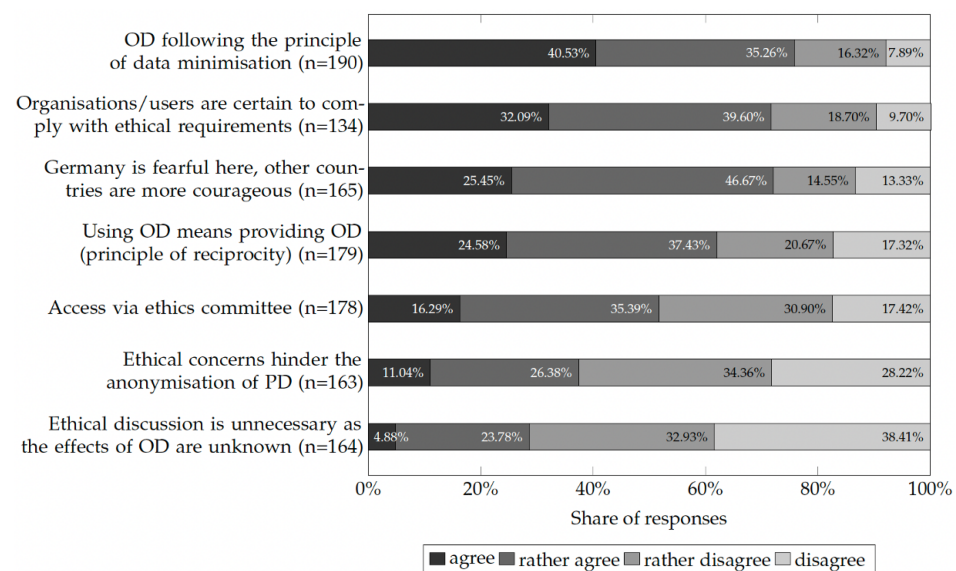


Figure 18. Perceived ethical implications of OD, including principles of minimisation, reciprocity, and oversight. Most respondents supported data minimisation (75.79%, $n = 144$ among $n = 190$ respondents) and reciprocity (62.01%, $n = 111$ among $n = 179$ respondents). Ethical concerns were not seen as a hindrance to anonymisation (62.58% disagreement, $n = 102$ among $n = 163$ respondents), and 71.34% ($n = 117$ among $n = 164$ respondents) rejected the view that ethical discussion is unnecessary.

4. Summary

This study yielded several important findings. A central research focus concerned how institutions and companies in Germany collect, process, and store PD in compliance with the GDPR, and which actors are primarily involved in these processes. The survey also examined barriers, support services, and specific ethical and legal aspects of anonymising PD, publishing it, and reusing it as OD.

All surveyed institutions and companies reported having access to PD. However, the high availability of PD combined with limited experience in anonymisation and reuse suggests that this resource remains underutilised. Most PD was collected and processed using both electronic and paper-based systems, which constrained subsequent data handling. Electronic processing was least standardised during data collection and only slightly increased in later phases. Many respondents were uncertain whether external parties could benefit from the data, reflecting limited awareness of reuse potential. Generally, PD was processed lawfully and exclusively for its original purpose, in line with GDPR provisions.

Regarding experiences with anonymisation, only a small proportion of institutions had previously anonymised PD and published it as OD. The key stakeholders identified in this process were data collectors, who typically also planned and implemented anonymisation. Data protection officers held supervisory roles, while IT departments provided technical support. Senior management and department heads were usually only informed. Nearly half of the respondents lacked an internal legal department, complicating legal assessments. Fixed responsibilities and formalised procedures were largely absent. Structured data were considered most relevant for anonymisation, followed by image and unstructured data, highlighting diverse potential applications. Respondents reported the strongest expertise in legal evaluation, structured data processing, and ethical or technical assessments, but notable gaps in knowledge regarding the anonymisation of unstructured and image data.

Experience with publishing anonymised data as OD was even more limited. Most respondents cited missing process standards and unclear responsibilities. Among those with publication experience, external requirements were the primary motivation. As in anonymisation, data-collecting departments led the process, supported by IT and supervised by data protection officers, while management was usually only informed. Publications most often appeared on institutional websites or governmental data portals. Most respondents reported no problems or adverse effects from publication.

Perceptions of OD revealed broad support for access and use restrictions, even though free availability was generally endorsed. Most participants considered anonymisation essential for future reuse. Opinions on licensing anonymised data were divided, with many opposing it or lacking sufficient knowledge to judge. The expected future importance of OD was also assessed inconsistently. Similarly, the majority of respondents had no prior experience with OD use. Although many expressed interest in expanding OD use, only a few institutions had internal OD initiatives or policies. Overall, the results indicated a weak organisational OD culture and low managerial expectations for increased adoption.

Major barriers to anonymisation and publication included high time and personnel demands, technical and institutional constraints, and ethical concerns about potential misuse of data. Competition resulting from OD provision was also viewed as an obstacle. The most requested support services were anonymisation software, followed by targeted training and expert consultation.

Regarding legal and ethical aspects, most respondents reported compliance with current legal requirements but expressed concern about future risks of re-identification arising from technological advances. Legal issues primarily concern the use of AI in data processing, with broad support for regulatory frameworks that balance AI's benefits and risks. Many respondents also supported access restrictions, clear liability rules for re-

identification, and a national supervisory authority for OD processes. However, most rejected a general obligation to inform data donors about anonymisation.

Ethically, the principle of data minimisation was regarded as highly important, as was the notion that OD provision should be linked to OD access (principle of reciprocity). Nevertheless, most respondents opposed the routine involvement of ethics committees. At the same time, participants emphasised the need for continuous ethical reflection on the societal impacts of OD use, arguing that ethical concerns should inform, but not hinder, the anonymisation and reuse of data.

5. Discussion

The available empirical data provides for the first time important information on institutional experiences in Germany with the anonymisation and publication process of previously personal data. This allows us to derive a series of recommendations for action, which we have grouped into the following categories: data collection and use, experiences with anonymisation and publication, obstacles and challenges, support services and capacity building, and legal and ethical considerations.

5.1. Data Collection and Utilisation

The first research question explored how PD are primarily collected and processed within the participating sectors. The study identified significant potential for data reuse, consistent with international evidence [1]. Although limited awareness of the benefits of OD was apparent, the results confirm the cross-sectoral value of such datasets for innovation and development. The findings also emphasise the importance of fully electronic data processing, not only to optimise collection but also to facilitate downstream handling, storage, and archiving, as confirmed by earlier studies [7]. Digital workflows enable broader analytical use and reduce spatial and personnel costs compared to paper-based systems. However, these processes must integrate robust cybersecurity and access control measures [15,37,38]. Limited internal experience with PD reuse, consistent with international research [37], further indicates a need to strengthen awareness of OD's potential added value through targeted information and training initiatives.

5.2. Experience with Anonymisation and Publication

The second research question examined existing experience with anonymisation and data publication. The survey revealed limited expertise in both areas. Uncertainty regarding the legal definition and application of anonymisation was common, as also reported elsewhere [6]. Despite some subjective expertise in law, technology, and ethics, systematic knowledge management is needed to update and consolidate institutional know-how [39,40]. Structured data were rated as most relevant for anonymisation, confirming prior findings [1]. Simplified and guided anonymisation procedures for these data types should therefore be prioritised. Anonymisation was typically carried out by departments that also collected the PD. This underscores the need to directly engage data protection officers, IT specialists, and management staff in training programmes on secure, technically supported anonymisation practices. Professionalisation of anonymisation further requires clearly defined responsibilities, procedural documentation, and integration into existing quality management systems [6]. The study aligns with international evidence highlighting the need for structured guidance and internal support mechanisms [1,39–42]. Experience with publishing anonymised data as OD was even scarcer. As with anonymisation, publication was mainly driven by contractual or legal obligations [43,44]. Expanding OD availability will therefore require embedding publication requirements within contracts, transparency regulations, and legal frameworks. Fixed responsibilities and procedural

structures for publication were largely absent. Given the overlap of personnel responsible for both anonymisation and publication, these actors—particularly data protection officers and IT staff—should receive comprehensive training and allocated resources. Improved access to suitable publication platforms, such as governmental OD portals, could enhance data dissemination beyond institutional websites [7].

5.3. Barriers and Challenges

The third research question focused on perceived barriers. The survey revealed significant deficits in time, personnel, technical resources, and procedural clarity [39,40,42]. Management support was often lacking, reflecting the absence of institutional OD policies or cultures. Respondents expressed a strong need for technical tools to simplify anonymisation and publication processes, consistent with earlier qualitative studies [6]. These challenges should be addressed through structured process design and the development of institutional OD strategies. The results also indicate a heterogeneous understanding of key terms such as “open data” and “anonymisation,” affecting perceptions of their benefits and implementation. A common conceptual framework is essential for improving acceptance and uptake. Ethical and legal concerns—particularly regarding re-identification risks and insufficient trust in current technologies—were identified as additional barriers [6]. Moreover, transparency regarding publication platforms and repositories remains limited, restricting data visibility and reuse. Despite general willingness to use OD, practical implementation remains rare. Respondents often perceived institutional OD initiatives as symbolic rather than effective, consistent with prior reviews [1]. Many potential users remain uncertain about the specific benefits of OD for their work, underscoring the need for more transparent communication and demonstration of practical value.

5.4. Support Services and Capacity Building

The fourth research question examined desired support services. The most frequently cited needs were governmental or institutional support through human, technical, and financial resources, consistent with international findings [7]. Respondents also called for research and development projects to create suitable technical tools. Training and knowledge transfer were identified as central elements for sustainable implementation [1]. Professional associations, research consortia, and networks such as chambers of industry and commerce should offer specialised training to strengthen institutional expertise and foster OD adoption. Recognised certification systems for anonymisation and publication processes were viewed as valuable instruments for enhancing trust and credibility [14,45,46]. To further promote transparency and trust, differentiated access models defining user rights and restrictions could also be implemented. Leadership and management play a crucial role in advancing anonymisation and OD publication—both as role models [7] and as providers of best practices [39]. Targeted training programmes for executives are therefore essential to establish a sustainable OD culture.

5.5. Legal and Ethical Considerations

The fifth research question addressed legal and ethical aspects of anonymisation and publication. Institutions must remain aware of the associated challenges and contribute to shaping appropriate governance frameworks [23]. Particular attention should be given to the implications of AI for OD analysis. Although the EU AI Act provides a comprehensive regulatory framework, respondents expressed concern about potential re-identification risks and called for explicit liability provisions [8]. The establishment of trusted supervisory authorities, such as the German Federal Office for Information Security (BSI), was also recommended to strengthen confidence in OD governance. Ethically, respondents emphasised the continued relevance of data minimisation and reciprocity—the principle

that OD provision should be linked to OD access. Established research ethics frameworks, such as the Declaration of Helsinki, may serve as guiding references for OD practices. Although most respondents opposed mandatory informed consent for anonymisation, they supported ongoing ethical reflection and, where appropriate, the involvement of ethics committees to enhance credibility and public trust. Overall, the results demonstrate that overcoming fears and uncertainties, building legal and ethical competence, and fostering trust are key prerequisites for the wider adoption of anonymised PD and OD in Germany.

6. Limitation

The study provides important first insights into the current state of knowledge regarding the anonymisation and publication of formerly PD as OD in Germany across the four involved sectors. However, several methodological, questionnaire, sampling, and data analysis limitations must be considered when interpreting the results.

6.1. Methodological Implementation

Data collection was carried out exclusively via an online questionnaire, which presupposes digital competence, internet access, and a certain level of self-motivation. Individuals who were less technically skilled or less interested in the subject may therefore have refrained from participating. Furthermore, participation was voluntary, which suggests a self-selection bias, as mainly individuals with an interest and prior experience in anonymisation and open data may have completed the questionnaire. More than half of the respondents were data protection officers, which may have influenced their perspectives on anonymisation and open data, particularly regarding data protection concerns specific to this professional group. The response rate of 0.53% was remarkably low, prompting critical reflection on both the recruitment strategy and the completion time of the online questionnaire. The extremely low response rate reduces the explanatory power of the results and distorts the findings. Thus, both response and attrition bias are likely. Possible reasons include the relatively long processing time due to the large number of categories and items (an estimated 25 min for 116 question-items), which may have led to fatigue and superficial responses. The Hawthorne effect cannot be ruled out, as participants with a strong interest in the topic may have been more willing to participate. Furthermore, limited expertise or low interest in the subject, as well as the perception that certain questions were irrelevant or imprecise, may have contributed to the high dropout rate. Consequently, many questions remained unanswered, or the survey was terminated prematurely. In addition, a gender bias may have affected the results, as 72% of respondents were male.

6.2. Questionnaire Development

During the development of the questionnaire, particular attention was paid to ensuring the relevance of the content, with all items derived from findings of the preceding scoping review and interview study. A pre-test was conducted to ensure clarity and relevance; however, no formal assessment of validity or reliability was carried out during questionnaire construction. Filter and control questions were used to guide participants in accordance with inclusion and exclusion criteria and their level of experience in anonymisation and open data. This provided a mechanism for plausibility-checking respondents' answers. Nevertheless, the questionnaire contained technical terminology whose precise understanding among participants could not be verified. Responses to open-ended questions indicated that terms such as anonymisation and pseudonymisation were sometimes used ambiguously or interpreted inconsistently. Since no follow-up interviews were conducted, such ambiguities or misunderstandings could not be clarified.

6.3. Sampling

Difficulties in recruiting professionals with sufficient expertise suggest that the chosen sampling strategy may have introduced bias. The crawling method used to generate the sample was limited to publicly accessible websites containing an email address in their legal notice (Impressum). Although providing a data protection contact address is a legal requirement in Germany, it is not consistently implemented. Thus, a non-probabilistic sampling strategy was applied, and only individuals with publicly available email addresses were included. Consequently, the crawling method produced a convenience sample, as only those whose contact details were publicly accessible and technically retrievable could be reached. This restricts the generalisability of the findings. In subsequent recruitment phases, snowball sampling was additionally employed. However, it was not possible to determine how often the survey link was forwarded internally or externally. This method aimed to increase the response rate, yet snowball sampling can further reinforce bias towards specific networks and professional groups. Systematic selection and attrition biases, particularly favouring participants with technical expertise, strong thematic interest, or voluntary self-selection, therefore cannot be excluded. Filter questions at the beginning of the questionnaire were intended to ensure compliance with inclusion and exclusion criteria within the snowball sampling process, although this could theoretically be bypassed if incorrect information was provided.

6.4. Limitations in Data Analysis

Including four sectors (business, research, public authorities, and healthcare) reduces statistical power. In terms of distribution, most respondents came from public administration and the private sector, while healthcare and research were underrepresented. A subgroup analysis and comparison between sectors were not statistically meaningful due to the small sample sizes in certain groups. Therefore, the results were analysed strictly descriptively, with the sample size reported for each item. This transparent approach reflects the study's measurement limitations and avoids unwarranted inferential conclusions. However, purely descriptive analysis does not allow causal interpretations. Owing to the cross-sectional design and single time point of data collection, no temporal developments can be assessed. Moreover, only about half of the respondents reported explicit experience with anonymisation processes. Approximately one quarter had experience with data publication. This further limits the generalisability of findings relating specifically to anonymisation and publication practices. Future studies should aim for larger sample sizes within individual sectors to enable more robust statistical analyses, particularly to test for potentially significant group differences. Sampling should be based on a probabilistic strategy to prevent under- or overrepresentation of specific sectors and to minimise the biases identified in this study. Additionally, longitudinal studies would be beneficial to monitor changes in experience with anonymisation and publication over time. Future research should also adopt a broader analytical perspective on contextual factors that may influence anonymisation and data publication practices. Despite limitations, the partial alignment of these findings with results from previous studies conducted in other countries indicates that the present study accurately reflects anonymisation and data publication practices within the German sample. Although the results are only partially transferable across all four sectors, the study highlights that similar challenges—such as the lack of technical tools or insufficient time and human resources—appear to exist in all four domains.

Supplementary Materials: The following supporting information can be downloaded at <https://www.mdpi.com/article/10.3390/info16121111/s1>.

Author Contributions: Conceptualization, N.L., S.W., F.W. and L.S.; methodology, N.L. and L.S.; software, S.W. and F.W.; validation, N.L., S.W., F.W. and L.S.; formal analysis, N.L. and L.S.; investigation, N.L. and S.W.; resources, F.W.; data curation, S.W. and N.L.; writing—original draft preparation, N.L., S.W., L.S. and F.W.; writing—review and editing, N.L., F.W., S.W. and L.S.; visualization, N.L. and S.W.; supervision, F.W.; project administration, S.W. and F.W.; funding acquisition, S.W. and F.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union and sponsored by the German Federal Ministry of Research, Technology and Space under grant number 16KISA128K (“Verbundprojekt: Empfehlungs- und Auditsystem zur Anonymisierung—EAsyAnon”).

Institutional Review Board Statement: In order to consistently and proactively rule out ethical and data protection concerns regarding the research project, an application was submitted to the Joint Ethics Committee of Bavarian Universities (GEHBa) prior to the start of the empirical accompanying research by EAsyAnon and was approved (No. GEHBa -202309-V-124).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: An anonymised version of all raw data and the corresponding SPSS syntax file are openly available free of charge via Zenodo at <https://doi.org/10.5281/zenodo.17571648>. Any additional materials containing potentially identifiable information can be obtained from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
CROSS	Checklist for Reporting of Survey Studies for Quantitative Methodology
DGA	Data Governance Act
EHDS	European Health Data Space
GDPR	General Data Protection Regulation
OD	Open Data
OHD	Open Health Data
OGD	Open Governance Data
PD	Personal Data

References

1. Lichtenauer, N.; Schmidbauer, L.; Wilhelm, S.; Wahl, F. A Scoping Review on Analysis of the Barriers and Support Factors of Open Data. *Information* **2024**, *15*, 5. [CrossRef]
2. Rehman, A.; Naz, S.; Razzak, I. Leveraging big data analytics in healthcare enhancement: trends, challenges and opportunities. *Multimed. Syst.* **2021**, *28*, 1339–1371. [CrossRef]
3. Kamikubo, R.; Lee, K.; Kacorri, H. Contributing to Accessibility Datasets: Reflections on Sharing Study Data by Blind People. In Proceedings of the CHI '23: 2023 CHI Conference on Human Factors in Computing Systems, Hamburg, Germany, 23–28 April 2023; ACM: New York, NY, USA, 2023; pp. 1–18. [CrossRef]
4. Mutambik, I.; Nikiforova, A.; Almuqrin, A.; Liu, Y.D.; Floos, A.Y.M.; Omar, T. Benefits of Open Government Data Initiatives in Saudi Arabia and Barriers to Their Implementation. *J. Glob. Inf. Manag.* **2022**, *29*, 22. [CrossRef]
5. Seo, J.; Kim, B.; Kwon, H.Y. Open Data Policies Analysis Disputes Mediation Cases in Korea: Based on OUR Data Index and ODB. In Proceedings of the DG.O'21: The 22nd Annual International Conference on Digital Government Research, Omaha, NE, USA, 9–11 June 2021; ACM: New York, NY, USA, 2021; pp. 153–167. [CrossRef]
6. Lichtenauer, N.; Guggemos, J.; Kampmann, M.; Kis, J.; Laumer, F.; März, E.; Wahl, F.; Wilhelm, S. Expert Experiences in Anonymizing Personal Data and Its Use as Open Data: Qualitative Insights. *Data* **2025**, *10*, 105. [CrossRef]
7. Kawashita, I.; Baptista, A.A.; Soares, D. Open gOvernment Data Use by the Public Sector—An Overview of Its Benefits, Barriers, Drivers, and Enablers. 2022. Available online: <http://hdl.handle.net/10125/79648> (accessed on 28 July 2025).
8. Crusoe, J.; Melin, U., Investigating Open Government Data Barriers: A Literature Review and Conceptualization. In *Electronic Government*; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 169–183.

9. Dos Santos Rocha, A.; Albrecht, E.; El-Boghdadly, K. Open science should be a pleonasm. *Anaesthesia* **2023**, *78*, 551–556. [CrossRef] [PubMed]
10. Eva, G.; Liese, G.; Stephanie, B.; Petr, H.; Leslie, M.; Roel, V.; Martine, V.; Sergi, B.; Mette, H.; Sarah, J.; et al. Position paper on management of personal data in environment and health research in Europe. *Environ. Int.* **2022**, *165*, 107334. [CrossRef]
11. Alzahrani, A.G.; Alhomoud, A.; Wills, G. A Framework of the Critical Factors for Healthcare Providers to Share Data Securely Using Blockchain. *IEEE Access* **2022**, *10*, 41064–41077. [CrossRef]
12. Medley, N.; Cuthbert, A.; Crew, R.; Stewart, L.; Smith, C.T.; Alfievic, Z. Developing a topic-based repository of clinical trial individual patient data: experiences and lessons learned from a pilot project. *Syst. Rev.* **2021**, *10*, 162. [CrossRef]
13. Queralt-Rosinach, N.; Kaliyaperumal, R.; Bernabé, C.H.; Long, Q.; Joosten, S.A.; van der Wijk, H.J.; Flikkenschild, E.L.; Burger, K.; Jacobsen, A.; Mons, B.; et al. Applying the FAIR principles to data in a hospital: challenges and opportunities in a pandemic. *J. Biomed. Semant.* **2022**, *13*, 12. [CrossRef] [PubMed]
14. Horn, R.; Kerasidou, A. Sharing whilst caring: solidarity and public trust in a data-driven healthcare system. *BMC Med. Ethics* **2020**, *21*, 110. [CrossRef]
15. Fylan, F.; Fylan, B. Co-creating social licence for sharing health and care data. *Int. J. Med. Inform.* **2021**, *149*, 104439. [CrossRef]
16. Bentzen, H.B.; Castro, R.; Fears, R.; Griffin, G.; ter Meulen, V.; Ursin, G. Remove obstacles to sharing health data with researchers outside of the European Union. *Nat. Med.* **2021**, *27*, 1329–1333. [CrossRef]
17. Viberg Johansson, J.; Bentzen, H.B.; Mascalzoni, D. What ethical approaches are used by scientists when sharing health data? An interview study. *BMC Med. Ethics* **2022**, *23*, 41. [CrossRef]
18. European Data Portal (Publications Office of the European Union). Open health data on the European Data Portal. In *Data Story, European Data Portal*; Publications Office der Europäischen Union: Luxembourg, 2019. Available online: <https://data.europa.eu/en/publications/datastories/open-health-data-european-data-portal> (accessed on 28 July 2025).
19. Feeney, O.; Werner-Felmayer, G.; Siipi, H.; Frischhut, M.; Zullo, S.; Barteczko, U.; Øystein Ursin, L.; Linn, S.; Felzmann, H.; Krajnović, D.; et al. European Electronic Personal Health Records initiatives and vulnerable migrants: A need for greater ethical, legal and social safeguards. *Dev. World Bioeth.* **2019**, *20*, 27–37. [CrossRef]
20. Hallock, H.; Marshall, S.E.; 't Hoen, P.A.C.; Nygård, J.F.; Hoorne, B.; Fox, C.; Alagaratnam, S. Federated Networks for Distributed Analysis of Health Data. *Front. Public Health* **2021**, *9*, 712569. [CrossRef]
21. Nellåker, C.; Alkuraya, F.S.; Baynam, G.; Bernier, R.A.; Bernier, F.P.; Boulanger, V.; Brudno, M.; Brunner, H.G.; Clayton-Smith, J.; Cogné, B.; et al. Enabling Global Clinical Collaborations on Identifiable Patient Data: The Minerva Initiative. *Front. Genet.* **2019**, *10*, 611. [CrossRef] [PubMed]
22. Avraam, D.; Jones, E.; Burton, P. A deterministic approach for protecting privacy in sensitive personal data. *Bmc Med. Inform. Decis. Mak.* **2022**, *22*, 24. [CrossRef] [PubMed]
23. Ethikrat, D. Big data und gesundheit—datensouveränität als informationelle freiheitsgestaltung. *Vorabfassung Vom* **2017**, *30*, 2017.
24. Mahomed, S.; Labuschaigne, M.L. The evolving role of research ethics committees in the era of open data. *S. Afr. J. Bioeth. Law* **2023**, *15*, 80–83. [CrossRef]
25. van Donge, W.; Bharosa, N.; Janssen, M.F.W.H.A. Future government data strategies: data-driven enterprise or data steward?: Exploring definitions and challenges for the government as data enterprise. In Proceedings of the dg.o '20: The 21st Annual International Conference on Digital Government Research, Seoul, Republic of Korea, 15–19 June 2020; ACM:New York, NY, USA, 2020; pp. 196–204. [CrossRef]
26. Kamocki, P.; Lindén, K. EU Data Governance Act: New Opportunities and New Challenges for CLARIN. In Proceedings of the CLARIN Annual Conference, Prague, Czechia, 10–12 October 2022; pp. 44–47.
27. Folz, J.; Aufschläger, R.; Vidanalage, M.D.; März, E.; Guggumos, J.; Uddin, M.M.; Wilhelm, S. Software Requirements Specification: EAsyAnon Recommender System. 2024. Available online: <https://zenodo.org/records/13318624> (accessed on 25 July 2025).
28. Folz, J.; Aufschläger, R.; Vidanalage, M.D.; März, E.; Guggumos, J.; Uddin, M.M.; Wilhelm, S. Software Requirements Specification: EAsyAnon Audit System. 2024. Available online: <https://zenodo.org/records/13734418> (accessed on 25 July 2025).
29. Schoonenboom, J. The Fundamental Difference Between Qualitative and Quantitative Data in Mixed Methods Research. *Forum Qual. Sozialforschung/Forum: Qual. Soc. Res.* **2023**, *24*, 11. [CrossRef]
30. Levitt, H.M.; Bamberg, M.; Creswell, J.W.; Frost, D.M.; Josselson, R.; Suárez-Orozco, C. Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA Publications and Communications Board task force report. *Am. Psychol.* **2018**, *73*, 26–46. [CrossRef]
31. Kuckartz, U. *Mixed Methods: Methodologie, Forschungsdesigns und Analyseverfahren*; Springer: Berlin/Heidelberg, Germany, 2014.
32. Helfferich, C., Leitfaden- und Experteninterviews. In *Handbuch Methoden der empirischen Sozialforschung*; Springer Fachmedien Wiesbaden: Berlin/Heidelberg, Germany, 2014; pp. 559–574. [CrossRef]
33. Buschle, C.; Bethmann, A. Kognitives Pretesting. 2017. Available online: <https://zenodo.org/records/997323> (accessed on 25 July 2025).

34. Schröder, A.; Proll, L.; In-Albon, T. Informed Consent in Onlinestudien: Wieviel verstehen Teilnehmende wirklich und lässt sich das ändern? *Z. Für Klin. Psychol. Und Psychother.* **2023**, *52*, 38–50. [\[CrossRef\]](#)
35. Forschungsgemeinschaft, D. Guidelines for Safeguarding Good Research Practice. Code of Conduct. 2025. Available online: <https://zenodo.org/records/14281892> (accessed on 25 July 2025).
36. Sharma, A.; Minh Duc, N.T.; Luu Lam Thang, T.; Nam, N.H.; Ng, S.J.; Abbas, K.S.; Huy, N.T.; Marušić, A.; Paul, C.L.; Kwok, J.; et al. A Consensus-Based Checklist for Reporting of Survey Studies (CROSS). *J. Gen. Intern. Med.* **2021**, *36*, 3179–3187. [\[CrossRef\]](#)
37. Nunes Vilaza, G.; Coyle, D.; Bardram, J.E. Public Attitudes to Digital Health Research Repositories: Cross-sectional International Survey. *J. Med. Internet Res.* **2021**, *23*, e31294. [\[CrossRef\]](#)
38. Kuo, T.T.; Jiang, X.; Tang, H.; Wang, X.; Harmanci, A.; Kim, M.; Post, K.; Bu, D.; Bath, T.; Kim, J.; et al. The evolving privacy and security concerns for genomic data analysis and sharing as observed from the iDASH competition. *J. Am. Med. Inform. Assoc.* **2022**, *29*, 2182–2190. [\[CrossRef\]](#)
39. Dove, G.; Shanley, J.; Matuk, C.; Nov, O. Open Data Intermediaries: Motivations, Barriers and Facilitators to Engagement. *Proc. Acm-Hum.-Comput. Interact.* **2023**, *7*, 1–22. [\[CrossRef\]](#)
40. Wolff, A.; Tylosky, N.; Hasan, T. Open data inclusion through narrative approaches. In Proceedings of the ICSE '22: 2022 ACM/IEEE 44th International Conference on Software Engineering: Software Engineering in Society, Pittsburgh, PA, USA, 21–29 May 2022; ACM: New York, NY, USA, 2022; pp. 125–129. [\[CrossRef\]](#)
41. Floridi, L.; Luetge, C.; Pagallo, U.; Schafer, B.; Valcke, P.; Vayena, E.; Addison, J.; Hughes, N.; Lea, N.; Sage, C.; et al. Key Ethical Challenges in the European Medical Information Framework. *Minds Mach.* **2018**, *29*, 355–371. [\[CrossRef\]](#)
42. Tuler de Oliveira, M.; Amorim Reis, L.H.; Marquering, H.; Zwinderman, A.H.; Delgado Olabarriaga, S. Perceptions of a Secure Cloud-Based Solution for Data Sharing During Acute Stroke Care: Qualitative Interview Study. *JMIR Form. Res.* **2022**, *6*, e40061. [\[CrossRef\]](#) [\[PubMed\]](#)
43. Beno, M.; Figl, K.; Umbrich, J.; Polleres, A. Perception of Key Barriers in Using and Publishing Open Data. *JeDEM—Ejournal Edemocracy Open Gov.* **2017**, *9*, 134–165. [\[CrossRef\]](#)
44. Ugochukwu, A.I.; Phillips, P.W. Open data ownership and sharing: Challenges and opportunities for application of FAIR principles and a checklist for data managers. *J. Agric. Food Res.* **2024**, *16*, 101157. [\[CrossRef\]](#)
45. Fischer-Hübner, S.; Alcaraz, C.; Ferreira, A.; Fernandez-Gago, C.; Lopez, J.; Markatos, E.; Islami, L.; Akil, M. Stakeholder perspectives and requirements on cybersecurity in Europe. *J. Inf. Secur. Appl.* **2021**, *61*, 102916. [\[CrossRef\]](#)
46. Sandoval-Almazan, R.; Valle Gonzalez, L.; Millan Vargas, A. Barriers for Open Government Implementation at Municipal Level: The Case of the State of Mexico. In Proceedings of the DG.O'21: The 22nd Annual International Conference on Digital Government Research, Omaha, NE, USA, 9–11 June 2021; ACM: New York, NY, USA, 2021; pp. 113–122. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.