Chronicling GDPR Transparency Rights in Practice

The Good, the Bad and the Challenges ahead

Pierre Dewitte, Jef Ausloos

International Data Privacy Law, Volume 14, Issue 1 <http://doi.org/10.1093/idpl/ipad026>

Supplementary materials and replication data available at:
<https://doi.org/10.48804/AB97EK>

Abstract.

- Transparency provisions, and the right of access in particular, have been an integral part of data protection law since the seventies but received a much-needed refresh with the General Data Protection Regulation (GDPR). Throughout the last few years, judicial and administrative authorities have clarified the scope and modalities of access, and a number of empirical studies have shed light the right has (not) been complied with in different contexts. So far, that empirical work has remained relatively disparate and hard to compare.

- This paper presents and compares the results of two legal-empirical studies conducted in 2020 and 2022 that were designed to gather quantitative and qualitative findings on how a selection of Online Service Providers (OSPs) have complied with their transparency obligations, and have answered access requests in practice. In doing so, it also provides a comprehensive overview of the most relevant soft law instruments, and provides all the supplementary materials necessary to replicate the research in an academic or educational context.

- These studies show that, while there have been substantial improvements on how OSPs handle access requests ("the good"), fundamental issues remain to be addressed ("the bad"). These include the widespread reliance on boilerplate answers, the routinisation of the process, the generic rather than specific nature of the information provided, and the lack of compliance with the default one month time limit. Addressing these shortcomings,

we argue, is critical in ensuring that controllers do not progressively erode the scope of Article 15 GDPR ("the challenges ahead").

Keywords. Compliance, Empirical study, GDPR, Transparency, Privacy policy, Right of access

I. INTRODUCTION

The General Data Protection Regulation (GDPR) became applicable on 25 May 2018.[1] Rarely has discourse on an EU legal instrument reached beyond law firms, legal departments, and academia. The GDPR, however, directly affected everyone. People were confronted with mushrooming cookie-consent banners across the web, uncertainties at work or their local sports club, and growing attention for data abuses in the media, notably exemplified by the Cambridge Analytica scandal.

The rise of the GDPR to popular consciousness also meant a heightened recognition of data subject rights, and in particular the right of access enshrined in Article 15. It is fair to say that this prerogative has become a much exercised right in the digital society, used by a wide variety of actors in many different contexts and for truly diverse purposes.[2] These range from individuals simply wishing to learn more about how their personal data are being processed on an *ad hoc* basis, to strategic and collective exercises designed to shed light on opaque digital infrastructures and their impact on people. Notably, the right of access has proven quite valuable for platform workers in the ride hailing industry,[3] to the eCommerce sector,[4] and academic researchers capitalising on it in data donation projects.[5]

With more data subjects requesting access to their personal data, or obtain more information on the ins and outs of the underlying processing activities, concerns have also emerged as to controllers' compliance with the GDPR. Several large technology companies have, for instance, rolled out data download functionalities that (narrowly) predefine the content and form of how

[1] 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) [2016] OJ L 119/1.
[2] See, for example: René Mahieu and Jef Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' (LawArXiv 2020) preprint app 1 <https://osf.io/b5dwm> accessed 7 July 2020.
[3] Worker Info Exchange, 'Historic Digital Rights Win for WIE and the ADCU over Uber and Ola at Amsterdam Court of Appeal' (4 April 2023) <https://www.workerinfoexchange.org/post/historic-digital-rights-win-for-wie-and-the-adcu-over-uber-and-ola-at-amsterdam-court-of-appeal> accessed 30 June 2023.
[4] noyb, 'Amazon Workers Demand Data-Transparency' (14 March 2022) <https://noyb.eu/en/amazon-workers-demand-data-transparency> accessed 30 June 2023.
[5] Jakob Ohme and Theo Araujo, 'Digital Data Donations: A Quest for Best Practices' (2022) 3 Patterns 100467.

access requests are responded to.[6] Anecdotal and empirical evidence also point to disproportionate delays in answering such requests, deliberate obfuscation and delaying strategies, incomplete responses, or even the absence of any reaction at all.[7] We have already conducted such empirical research back in 2017, right before the GDPR became applicable, but after the EU legislator had adopted the final text (i.e., May 2016).[8] That work identified structural issues with how the right of access was (not) accommodated in practice. To quantify and document the impact of the GDPR on controllers' behaviour, we decided to undertake similar experiments in both 2020 and 2022, the outcome of which we analyse in this contribution.

This paper builds on and complements earlier empirical studies by gauging controllers' compliance with the right of access at two specific points in time since the GDPR became applicable.[9] In doing so, it builds on earlier work by the authors, as well as similar empirical studies conducted in the past five years.[10] It also embeds the empirical findings into the rapidly developing body of regulatory guidance on the right of access in Europe. While the findings may not surprise those familiar with the ins and outs of the right of access, we strongly believe that recurring quantitative and qualitative evidence is essential to keep data subjects, controllers, regulators, and policymakers informed about the state of access in practice. This, in turn, can help identify the areas for which efforts and/or guidance are still needed. Especially considering that our findings consistently point to significant undercompliance across the board. This paper also

[6] For instance, Jef Ausloos, René Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC <http://www.jipitec.eu/issues/jipitec-10-3-2019/5031>.

[7] See notably: Adamu Adamu Habu and Tristan Henderson, 'Data Subject Rights as a Research Methodology: A Systematic Literature Review' (2023) 16 Journal of Responsible Technology 100070.

[8] Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipy001/4922871> accessed 16 May 2023.

[9] Notable other studies, with slightly different scopes include: René Mahieu and others, 'Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?' (2021) 11 Journal of Information Policy 301; Jacob Leon Kröger, Jens Lindemann and Dominik Herrmann, 'How Do App Vendors Respond to Subject Access Requests? A Longitudinal Privacy Study on iOS and Android Apps', *Proceedings of the 15th International Conference on Availability, Reliability and Security* (Association for Computing Machinery 2020) <https://dl.acm.org/doi/10.1145/3407023.3407057> accessed 24 November 2023.

[10] See, for instance: Anna Ida Hudig, Chris Norval and Jatinder Singh, 'Transparency in the Consumer Internet of Things. Data Flows and Data Rights' (2023) <https://www.iot-transparency.org/> accessed 16 May 2023; Habu and Henderson (n 7); Mahieu and others (n 9); Plixavra Vogiatzoglou and others, 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives' (2021) 11 JIPITEC <https://www.jipitec.eu/issues/jipitec-11-3-2020/5191>; Ana Pop Stefanija and Jo Pierson, 'Practical AI Transparency: Revealing Datafication and Algorithmic Identities' (2020) 2 Journal of Digital Social Research 84; Janis Wong and Tristan Henderson, 'The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR' (2019) 9 International Data Privacy Law 173.

provides all the materials used to gather and analyse the empirical findings, which can be used, for instance, to replicate the methodology or as the basis for a teaching module.

II. FROM 2016 TO 2022: ACCESS, REVITALISED

The right of access has long been anchored in data protection law and can be historically conceptualised as "a way to empower people in relations characterized by structural informational power asymmetry".[11] It is a constitutive element of the fundamental right to data protection (Article 8(2) Charter) and has been an integral part of data protection laws since the 1970s.[12] Even so, compliance with the right of access has remained relatively low, and rarely led supervisory authorities to exercise their investigative and corrective powers.[13] Unsurprisingly therefore, one of the European Commission's explicit goals when proposing a data protection law overhaul in 2012 was to 'make the exercise of data protection rights by individuals more effective'.[14] That is why the GDPR now lays down specific requirements on how controllers should accommodate data subject rights, including the right of access. Notably, Article 12 states that controllers must answer such requests within one month and free of charge. Additionally, the GDPR also introduced much more potent enforcement capacity, with a strong mandate for DPAs to investigate and issue fines.[15] Importantly, the GDPR also introduces an option for Member States to constrain data subject rights (Article 23), but only under strict requirements and subject to a proportionality and necessity test. Any such restrictions ought to be interpreted narrowly,[16] and cannot undermine the rights conferred by the Charter of Fundamental Rights of the European

[11] A comprehensive overview of the history behind the right of access can be found in: René Mahieu, 'The Right of Access to Personal Data: A Genealogy' (2021) 2021 Technology and Regulation 62, 63.
[12] Ausloos and Dewitte (n 8) 4; Mahieu (n 11) 62.
[13] René Mahieu, 'The Right of Access to Personal Data in the EU' (PhD Thesis, Vrije Universiteit Brussel 2023) respectively 13 and 261-269 <https://researchportal.vub.be/en/publications/the-right-of-access-to-personal-data-in-the-eu-a-legal-and-empiri> accessed 25 October 2023.
[14] European Commission, 'Proposal for a Regulation of the European Parliament and of The Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' (25 January 2012) 4.
[15] The European Commission recently announced that it would take action on streamlining the cooperation between DPAs when enforcing the GDPR in cross-border cases. The Commission received 73 responses to its call for evidence. See: European Commission, 'Further Specifying Procedural Rules Relating to the Enforcement of the General Data Protection Regulation' (2023) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation> accessed 26 June 2023. On 4 July 2023 it proposed a new Regulation suggesting a set of harmonised procedural rules for the DPAs when applying the GDPR. See European Commission, 'Proposal for a Regulation of the European Parliament and of The Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 (4 July 2023).
[16] European Data Protection Board, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' para 3 <https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf> accessed 22 October 2021.

Union (the Charter), like the fundamental right to data protection that explicitly includes the right of access (Article 8(2) Charter).[17]

The applicability of the GDPR has triggered a surge of access requests.[18] Because of its functional simplicity, Article 15 is one of the most prominent tools granting individuals the possibility to observe complex digital infrastructures and expose opaque data practices. As mentioned above, it has proven useful to many different (groups of) people in the pursuit of various purposes. Its polyvalence, once heavily criticised, is now recognised by most as its main asset. Controllers appear to gradually acknowledge that as well, often offering more explicit ways of exercising the right of access and sometimes implementing (semi-) standardised ways of accommodating that right, notably through data download packages.

Early in 2023, the European Data Protection Board (EDPB) also published its updated Guidelines on the matter, which have confirmed most of what case law and scholars had already pointed out.[19] Notably that data subjects cannot be required to motivate their request or submit it in a specific format, as well as the fact that the right of access covers more than only a copy of one's personal data but also includes information about the processing operations that should be tailored to the specific situation of the data subject exercising their right. The EDPB also clarified that controllers have a duty to implement necessary measures to accommodate such requests and cannot reject these simply because they designed their infrastructures in a way that makes it hard to comply.[20]

Even though the GDPR and its accompanying soft law instruments have overall improved the state of data protection since Directive 95/46, uncertainties remain as to the exact scope and modalities of the right of access. This can be explained by a variety of factors, not in the least the formidable power asymmetries and complexities of data ecosystems that challenge both effective exercises of the right, as well as how they are (not) accommodated. Over the past few years, regulators and academics have tried to map and document these concerns in different ways. This paper builds on a comprehensive analysis of the most relevant soft-law instruments and scholarly literature to shed light on the current state of the right of access.

In our earlier work, we identified four fundamental flaws in the way controllers acted upon access rights. [21] First, a general lack of awareness as to the existence and scope of the right of access.

---

[17] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* [2020] ECLI:EU:C:2020:791, para 210.
[18] See, on that point, René Mahieu 'The Right of Access to Personal Data in the EU' (n 13) 255-256.
[19] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en> accessed 16 January 2023.
[20] ibid respectively 10, 52, 113-122 and 127-131.
[21] Ausloos and Dewitte (n 8) 16–18.

Second, a systematic lack of internal procedures and organisation to deal with such requests. Third, a recurring lack of motivation translating in extensive delays and irritated responses. Lastly, a lack of harmonisation inherent to the nature of Directive 95/46 that required data subjects to consider the requirements emanating from different national implementing laws before submitting their requests. Looking ahead, we expected that the introduction of the GDPR would improve compliance with the right of access thanks to 'clearer, well-defined and harmonized practical modalities'. The goal of the present paper is therefore to document whether controllers have improved on these aspects by reporting on two legal-empirical studies organised in, respectively, 2020 and 2022. As demonstrated below, our assumption only partially holds true.

The empirical evidence presented below is valuable for different actors. Firstly, and most importantly, it can help data subjects in managing expectations and anticipating specific hurdles to (individual or collective) exercises of the right. Secondly, we hope to encourage controllers to adjust their internal compliance strategies, including rethinking their collaborations with third party vendors offering compliance tools.[22] Thirdly, and to the extent controllers do not spontaneously improve their compliance routine, we also consider this empirical data relevant for data protection authorities when drafting relevant guidance, and amp up strategic enforcement efforts. Finally, the results may also be interesting for policymakers when designing new legal frameworks setting up similar requirements on those in control over data infrastructures.[23]

While we acknowledge the emergence of a vast body of administrative and judicial cases at Member State level,[24] the scope of this contribution did not allow for including a comprehensive analysis of these cases. That said, we do refer to relevant CJEU case law, which has clarified the scope and implications of some of the most important modalities of the right of access, such as what exactly is to be included in 'a copy of the personal data undergoing processing' (Article

[22] See, *e.g.*, the list of "Privacy Tech Vendors" established by the International Association of Privacy Professionals (IAPP) [2022] <https://iapp.org/resources/article/privacy-tech-vendor-report/> accessed 30 June 2023. See also Cristiana Santos and others, 'Consent Management Platforms Under the GDPR: Processors and/or Controllers?' in Nils Gruschka and others (eds), *Privacy Technologies and Policy* (Springer International Publishing 2021).
[23] Examples include the proposed Data Act (*e.g.*, Article 4), and the Digital Services Act (*e.g.*, Article 40).
[24] Including, among many other landmark cases, the fine issued by the Swedish Data Protection Authority (IMY) against Spotify for failing to provide users with sufficiently clear information, and the Dutch judicial saga involving Uber and Ola recently settled by the Amsterdam Court of Appeal on the interpretation of the so-called "right to explanation". See Integritetsskydds myndigheten, Sanktionsavgift mot Spotify [2023] <https://www.imy.se/nyheter/sanktionsavgift-mot-spotify/> accessed 30 June 2023. For the three decisions from the Amsterdam Court of Appeal, see: Gerechtshof Amsterdam, ECLI:NL:GHAMS:2023:793 [2023] <https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:GHAMS:2023:793> accessed 30 June 2023; Gerechtshof Amsterdam, ECLI:NL:GHAMS:2023:796 [2023] <https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:GHAMS:2023:796> accessed 30 June 2023; Gerechtshof Amsterdam, ECLI:NL:GHAMS:2023:803 [2023] <https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:GHAMS:2023:803> accessed 30 June 2023.

15(3)),[25] the obligation to share the identity of the actual recipients of the personal data (Article 15(1)c),[26] or prohibiting the right of access being made conditional on a motivation (*e.g.*, to be aware of and verify the lawfulness of the processing).[27]

III. EMPIRICALLY TESTING THE RIGHT OF ACCESS

This section sheds light on the methods, constraints and main resources used in our empirical study. Where relevant for either validation of replicability purposes, these resources are included as supplementary materials.

Methodology

The goal of the two-stage legal-empirical study presented below is to assess how controllers behave over time when confronted with access requests that seek to obtain all the elements listed in Article 15(1) GDPR. These studies were organised, respectively, in summer 2020 and 2022. Both involved around 70 online service providers (OSPs) and were conducted by students of the Master of Information Law organised by the Universiteit van Amsterdam ,[28] *together with* and under the direct *supervision of* the authors.[29]

First, the authors drafted questionnaires designed to capture both quantitative and qualitative evidence of controllers' compliance with transparency and data subject's rights, using the relevant legal provisions and soft law instruments as reference points. These were later implemented using Typeform, as the platform allows to extract the results in a machine-readable format.[30] Before each study, the authors organised a session to inform the students about the different steps of the process, discuss the timeline of the project, and adopt a common approach to standard scenarios. During that session, the authors also agreed, together with the students, on a selection of popular OSPs and equitably shared the workload. The final choice of OSPs aimed to include a mix of both established market players in their respective domains, as well as lesser knows services used by the participants. Figure 1 provides an overview of the sectors investigated in both 2020 and 2022.

[25] Case C-487/21 *FF v Österreichische Datenschutzbehörde* [2023] ECLI:EU:C:2023:369, paras 18-45.
[26] Case C-154/21 *RW v Österreichische Post AG* [2023] ECLI:EU:C:202, paras 39-42.
[27] Case C-307/22 *FT v DW* [2023] ECLI:EU:C:2023:811, para 43.
[28] The full programme of the Master of Information Law can be accessed at the following address: <https://www.uva.nl/programmas/masters/informatierecht/studieprogramma/studieprogramma.html> accessed 23 December 2023.
[29] "Participants", in that sense, include both the "authors" of this paper and the "students".
[30] The Typeform platform can be accessed at the following URL: <https://www.typeform.com>.

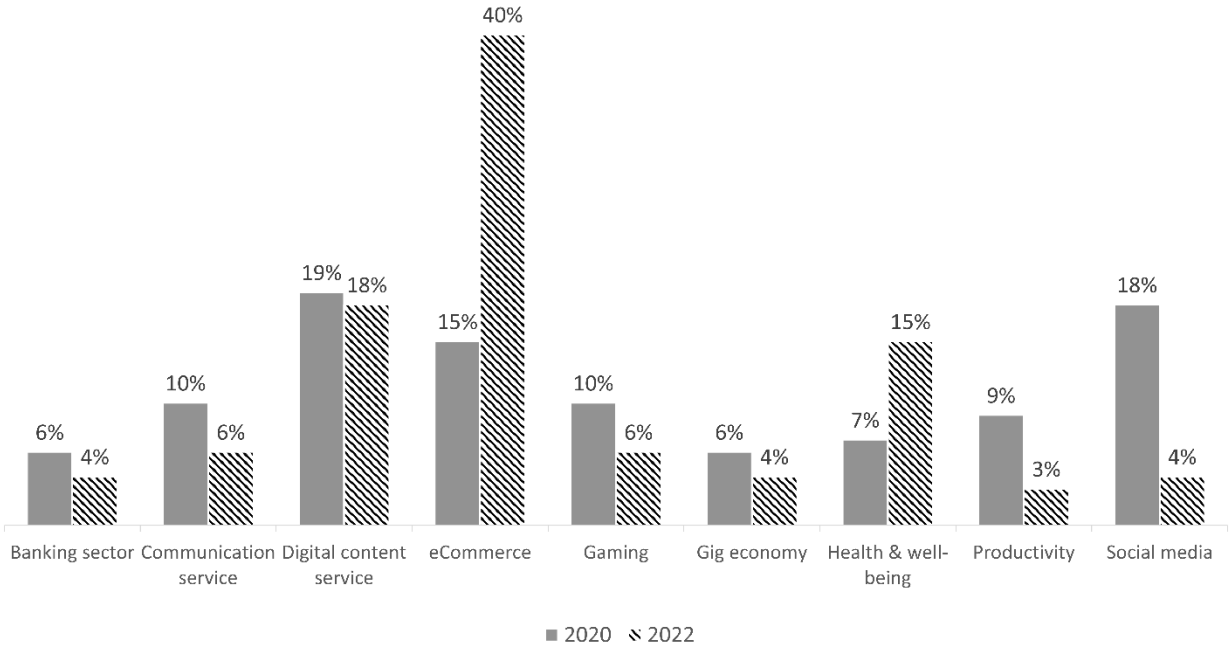

Figure 1 - Overview of the OSPs investigated

The actual studies took place in four steps, at the end of which the participants filled the corresponding Typeform survey to report on their findings. First, we registered and used the assigned OSPs for a certain period to fuel our profile with user data. Secondly, we looked for and went through each OSP's privacy, or data policy to evaluate both its content and its form, and searched for information as to how to exercise rights under Article 15-22 GDPR. Thirdly, we filed an initial, basic access request using the means referenced in the privacy/data policy, with the aim of gauging controllers' first reaction when confronted to an individual exercising his or her rights under the GDPR. We did not, at any point, indicate that our request would feed into this empirical study. Lastly, and in those cases where OSPs did answer to that initial request, we compared the content of that answer with the elements listed in Article 15(1) and – at least for the second study – in the draft EDPB Guidelines 01/2022, and engaged with the controller to obtain any missing information.

To ensure the validity of the quantitative results, especially when it comes to calculating the delays between controllers' answers, we all agreed on a strict reminder policy prior to the start of the study. We also organised regular calls to discuss and overcome hurdles faced along the way and align our reaction when confronted to certain scenarios (*e.g.*, what to do when a controller merely refers to its privacy/data policy or argues that a copy of the personal data can only be obtained through a self-service tool that is not comprehensive enough). Eventually, the strategy for approaching the follow-up stage was left up to each participant. While the goal was to stay general and try to obtain all the elements listed in Article 15(1) GDPR, this was not always

possible. As noted by the EDPB, "where the controller processes a large quantity of data concerning the data subject", there is an inherent tension between exhaustiveness and meaningfulness that can justify the controller asking the data subject to specify "the information or processing to which the request related before the information is delivered".[31] In these cases – and provided that the request for more precision was not used by the controller as a delaying tactic – the participants were free to decide which specific elements to target, taking into account the type of OSP as well as the aspects already under investigation by the other participants.[32]

Resources

Two types of supplementary materials come bundled with this article. First, the templates drafted by the authors and used throughout the course of both studies to exercise the right of access. More specifically, these include: (i) the template used to send the initial access requests, (ii) the template used to remind controllers of pending access requests, and (iii) the template used to request more information in cases where controllers came up with lacunary answers. Besides, we also share the four surveys used to report on the experiences in requesting access. The answers to these surveys, collected at various stages of the empirical studies, are the raw materials on which we crunched the numbers and crafted the various Figures presented in this paper. The four surveys concern, respectively: (i) the selection of and registration of the investigated OSPs, (ii) the assessment of their privacy/data policy, (iii) the submission of the initial access request and (iv) the follow-up process. The surveys are available in both .docx and .json format, which makes it convenient to replicate our methodology should one opt for a compatible survey service such as Typeform. The supplementary materials can be downloaded a the following URL, which contains all the necessary replication data: https://doi.org/10.48804/AB97EK.

We believe that these resources provide all the necessary building blocks for others to conduct similar studies in an academic or educational context. This could, for instance, help contribute to an incrementally growing body of comparable empirical research mapping compliance with data subject rights across the EU. A crucial research endeavour considering the wide diversity of existing empirical studies. It may also prove useful in setting-up dedicated thesis tracks or serve as a basis for the organisation of a teaching module in a variety of courses across different disciplines. Looking at the other end of the spectrum, the questions raised in the surveys could

[31] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 35 b). See also Recital 63 GDPR.

[32] Assessing whether controllers acted in good faith when asking to specify a broadly-formulated access request was left up to each participants, using agreed-upon indicators such as the size of the controller, the breath of its processing activities as reflected in its privacy/data policy, the disparities between the personal data collected by the service and that included in the controller's reply, and the tone used in its answer.

also help controllers identify areas in which additional efforts might still be required, and anticipate the types of requests they could be confronted with in the future.

Limitations

It is also important to acknowledge the limitations of our approach. First, we decided not to disclose the identity of the investigated OSPs. Our goal is not to name and shame, but rather to identify the main areas where compliance with data subject's rights is still lacking in general. This makes it impossible to strictly reproduce our experimental setting but does not affect the validity of the findings nor the robustness of our empirical methodology.

Second, the OSPs investigated in 2020 are not entirely the same as the ones scrutinised in 2022. Considering the limited sample size (*i.e.*, approximately 70 OSPs for each iteration), some differences between the results of 2020 and 2022 may be attributable to the choice of providers, rather than to a change of attitude towards compliance in general. The risk of accidental "bad samples" is, however, inherent to any kind of empirical research.

Third, the filled-in surveys are not included as part of the supplementary materials, since filtering out the personal data contained therein would involve disproportionate efforts, and largely deprive the findings of their added value. Where relevant, we refer to the qualitative findings directly in the text and present an overview of the quantitative results through dedicated Figures.

Fourth, as with all surveys designed to gather participants' opinions on a given topic, either through Likert scale or open observations, the results suffer from an inherent degree of subjectivity. In our case, it is also worth noting that all the participants were law students who had followed an entire course on EU data protection law. Both the quantitative and qualitative findings presented in this paper should therefore be understood as reflecting the opinion of individuals who may be more knowledgeable and critical than the average data subject.

Fifth, both studies were conducted before the adoption of the final version of the EDPB Guidelines 01/2022 on the right of access, which were nonetheless made available as a draft for public consultation halfway through the 2022 study. While we abundantly refer to these Guidelines in the remainder of this Section, the reader should bear in mind that the participants, especially back in 2020, could not have anticipated their content. Both iterations, however, took full advantage of the WP29 Guidelines on transparency when assessing controllers' compliance with their obligations under Articles 12-14 GDPR.[33]

[33] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' <https://ec.europa.eu/newsroom/article29/redirection/document/51025> accessed 16 January 2023.

Lastly, both the 2020 and 2022 empirical studies were conducted during the summer period, *i.e.*, from May until September. It is worth noting that some controllers might have been operating with reduced staff, which could potentially have affected the findings presented below, especially when it comes to compliance with the applicable time limits. Still, shortage of staff is no excuse for delays in answering access requests, and that circumstance is unlikely to have poisoned the overall conclusions drawn from our experience.

IV. THE LONG AND WINDING ROAD TO ACCESS

The presentation of the results is structured around the path data subjects will naturally follow when requesting access to their personal data, *i.e.*, i) read the privacy/data policy, ii) filing the access request, iii) correspond with the controller, and iv) assess the quality of the final answer. For each of these steps, we detail the applicable provision(s), provide an overview of the guidance on the matter, refer to the relevant recent cases from the CJEU if any, and report on controllers' compliance based on the qualitative and quantitative results of the legal-empirical study.

Assessing the Privacy/Data Policy

The privacy/data policy is the most common manifestation of controllers' obligation to ensure the transparency of their processing operations (Articles 5(1)a, 12-14 GDPR).[34] It is the first source of information data subjects will turn to when trying to understand how their personal data are processed. As such, a clear and comprehensive document will go a long way in keeping access requests to a minimum. In case data subjects still have questions left unanswered, the privacy/data policy also contains the information necessary for them to give effect to the arsenal of prerogatives granted by the GDPR.[35] Besides, it also serves as a basis to identify any discrepancy with the information provided by the controller following an access request. It is therefore crucial that controllers make it accessible, comprehensive, and understandable.

[34] If not the only one, that is. As noted by the Article 29 Working Party in its Opinion on transparency, "[t]he GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller's responsibility to take "appropriate measures" in relation to the provision of the required information for transparency purposes". See ibid 24. In the context of this paper, the term "privacy/data policy" refers to all form of privacy- and data protection-related information, regardless of its form and denomination.

[35] As noted by Advocate General Cruz Villalon in the *Bara* case, "the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive". See Case C-201/14 *Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others* [2014], Opinion of Advocate General Cruz Villalon, ECLI:EU:C:2015:461, para 74.

Accessibility

Given the role of *ex ante* transparency in enabling the exercise of data subject's rights,[36] Article 12(1) and Recitals 39 and 58 GDPR require controllers to "take appropriate measures to provide [...] any information referred to in Articles 13 and 14 in a[n] easily accessible form". According to the WP29, "the data subject should not have to seek out the information", but it should "be apparent to them where and how" to retrieve it.[37] That requirement is device-agnostic, although its concrete implementation will inevitably vary. For websites, the WP29 recommends controllers to display a direct link to their privacy/data policy at the bottom of each page using an unambiguous title.[38] App developers, on the other hand, are advised to "ensure that the information is never more than 'two taps away'" from the screen the user is currently browsing.[39]

The vast majority of privacy/data policies (77% in 2020 and 93% in 2022) could be accessed in one or two interactions (fig. 2).[40] Still, participants rated the process of finding that document "difficult" or "very difficult" for 6% (in 2020) and 8% (in 2022) of OSPs. This can be attributed to a number of factors, including the use of "infinite scrolling" that made it hard if not outright impossible to reach the bottom of the page, broken URLs, and the confusing bundling of that information with other legal or non-legal documents such as the "Terms & Conditions" or the "FAQ".[41] In some cases, participants regretted that the privacy/data policy was split into multiple parts accessible through dedicated URLs, with no way of getting either a summary or the full document in one single place. As recalled by the WP29, the adoption of a "layered" approach, while considered as a good practice in complex settings, should not prevent data subjects from the possibility to access to the complete document.[42]

---

[36] On the "enabling" role of the right of access, see: Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009], ECLI:EU:C:2009:293, para 51; Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017], ECLI:EU:C:2017:994, para 57.

[37] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) para 11.

[38] As noted by the Working Party, "provide" is the operative word in this context. See: ibid 11; 33.

[39] The Working Party does not, however, give any indication as to whether this should be understood *literally* as meaning that data subjects should, when using *mobile applications*, be able to reach the privacy/data policy is *no more than two interactions* with their device.

[40] It is worth noting that the modalities for accessing the privacy/data policy might very depending on the interface through which data subjects access the relevant service. To avoid testing each environment the OSPs were available on, we first asked participants to indicate the interface that data subjects were the most likely to use when accessing the service. In cases where there was a clear preference for a specific interface, we measured the accessibility of the privacy/data policy on that environment. In case of multiple relevant environments, we tested them all, referred to the best result in the survey, and detailed any noteworthy difference at the end of the corresponding survey.

[41] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) para 8.

[42] ibid 17, noting that "the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them".

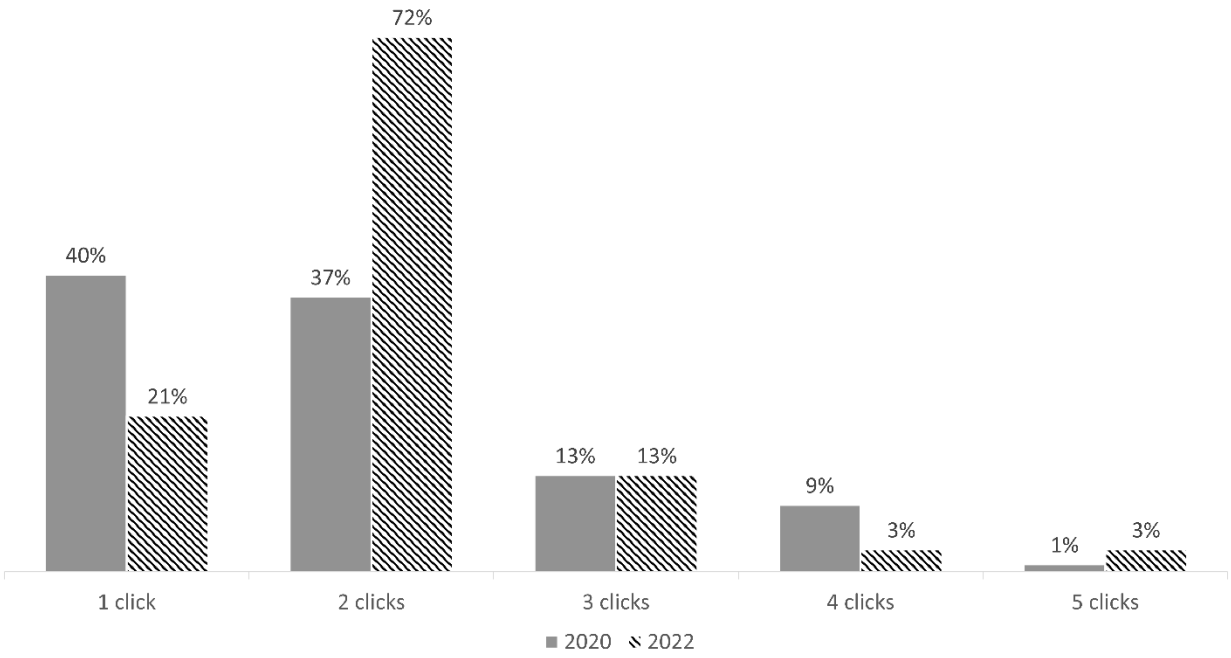

Figure 2 - Interactions needed to access the privacy/data policy

If data subjects must always be able to easily access the privacy/data policy, controllers are also expected to advertise the existence of that document at the latest when collecting the personal data at stake. A significant majority of OSPs did so, mostly through contextual pop-ups pointing at the relevant URL or mandatory read-through requiring some form of positive action from the data subject. Some controllers (16% in 2020 and 21% in 2022), however, failed to provide any privacy or data protection related information during the registration process or when using the service for the first time. This is particularly problematic for processing based on Article 6(1)a GDPR, as failure to redirect the data subject to the privacy/data policy or to at least provide an overview of the most important elements necessary to make an informed choice *prior to the actual collection* will likely poison the validity of the resulting consent. The accessibility component therefore plays an even more critical role in that context.[43]

Content

Articles 13 and 14 GDPR list the information that controllers must provide data subjects upfront.[44] Article 13 applies where personal data are collected directly from the data subject, whether

[43] See, on the impact of the accessibility of the privacy/data policy in the context of Article 6(1)a GDPR: European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' para 69 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 15 January 2023.

[44] For more details on each of these elements, see the Annex of Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) 35–40. We did not, however, keep track of whether OSPs

through observation or because the data subjects actively provided the said data, while Article 14 deals with the situation where personal data have not been obtained from the data subject but from third parties, publicly available sources, data brokers or even other data subjects. In case of data not obtained directly from the data subject, Article 14(3) GDPR states that the said information must be made available "within a reasonable period after [the controller] obtained the personal data", "at the time of the first communication with the data subject" or "when the personal data is first disclosed", but in any case "no later than one month" after the data have been obtained.[45] Content-wise, Article 14 GDPR is nearly identical to Article 13, if for the logical inclusion of the categories and sources of personal data in Article 14 GDPR. Regardless, the WP29 is of the opinion that there is "no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively",[46] and we also assumed such while conducting our legal-empirical study.

In 2022 we observed a notable increase in the amount of OSPs that provided information as to the lawful grounds used to justify their processing operations, from 79% to 90% (fig. 3). This is particularly welcome, as the choice of lawful ground determines some of the rights data subjects can exercise over the corresponding processing (*e.g.*, the right to withdraw their consent or to object to a processing based on Article 6(1)e and f).[47] Information on transfers and their accompanying safeguards was, however, still missing from many of the investigated privacy/data policies (28% in 2020, and 25% in 2022). When present, that information was not always up to date, with some OSPs still referring to the Privacy Shield in 2022,[48] for instance. On a more positive note, we noted an overall surge in OSPs that provided complete and accurate information on the existence of data subject's rights (fig. 4). This is particularly the case when it comes to the right to data portability (from 54% in 2020 to 87% in 2022), and the possibility to lodge a complaint with a supervisory authority (from 74% in 2020 to 96% in 2022).

provided any information on the "risks, rules, safeguards and rights in relation to the processing of personal data" as suggested by Recital 39. This is an integral part of the broader principle of "accountability" (Article 5(2)), and should transpire from the mandatory elements to be provided as per Article 13 and 14. See, specifically on that point, ibid 10, 28, 42.

[45] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) para 27. When it comes to personal data directly obtained from the data subject, Article 13(1) GDPR requires controllers to provide the necessary information "at the time when personal data are obtained".

[46] ibid 23.

[47] See, on that note, Ausloos, Mahieu and Veale (n 6) paras 71, 120–122.

[48] Even though the framework was struck down by the CJEU in July 2020. Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* [2020] ECLI:EU:C:2020:559.

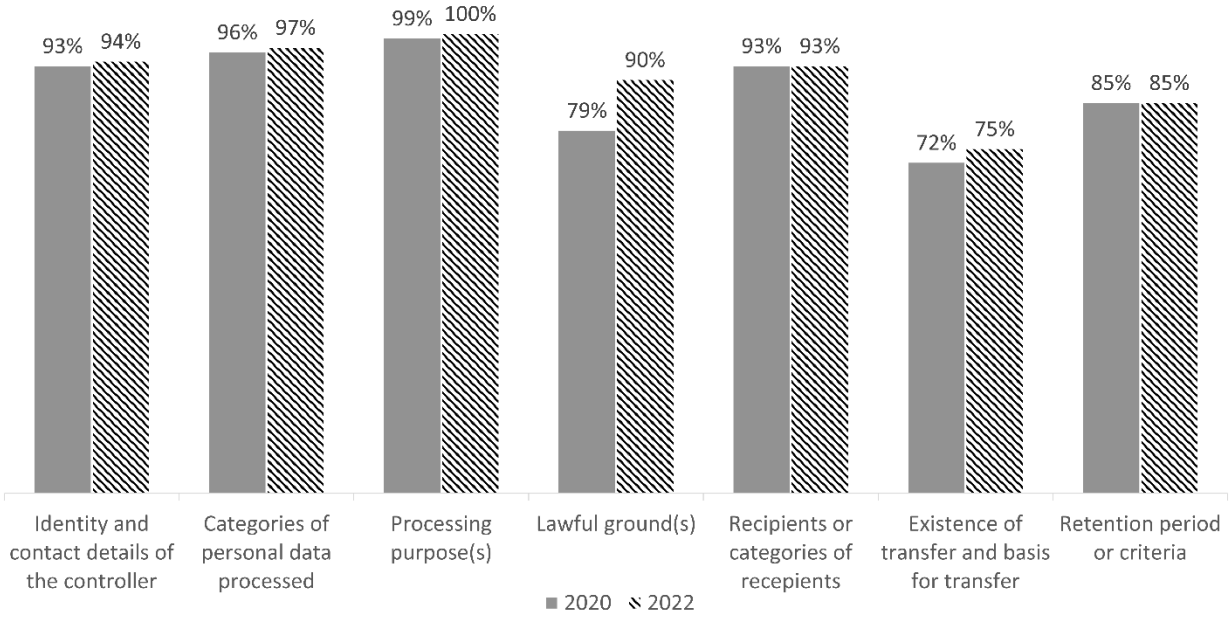

Figure 3 - Information provided in the privacy/data policy (1)

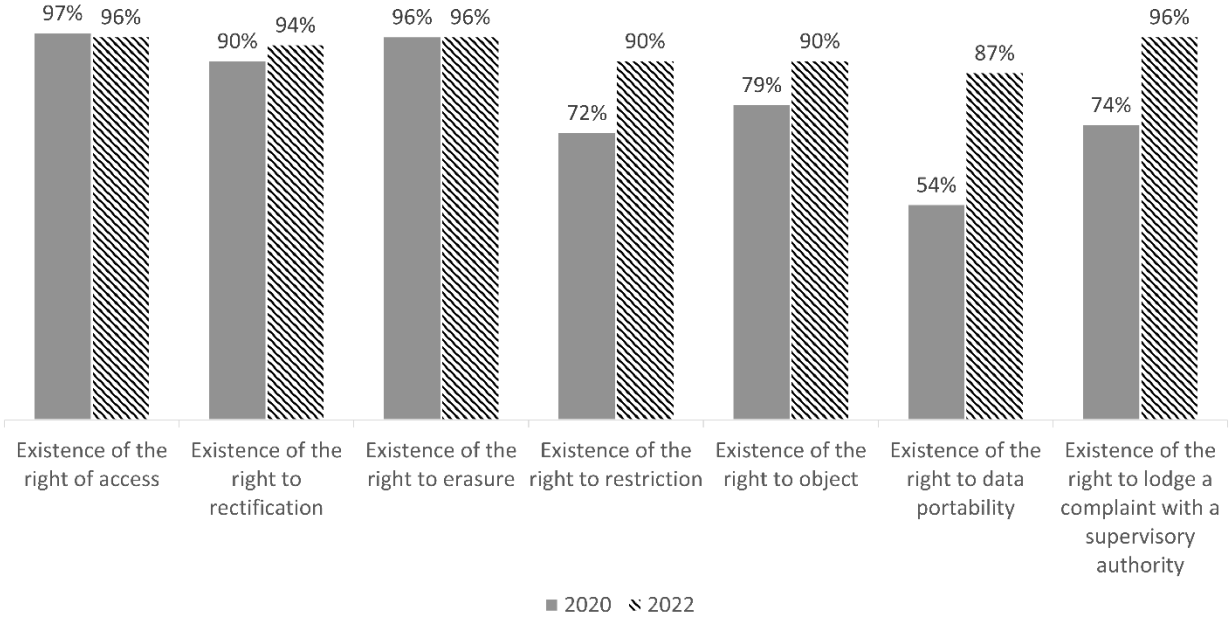

Figure 4 - Information provided in the privacy/data policy (2)

These improvements are reflected in the overall satisfaction rate for the content of the privacy/data policy, as 26% and 51% of participants considered it, respectively, “very satisfying” and “satisfying” (compared to 6% and 43% in 2020). Among the most often cited good practices, participants reported that some controllers explicitly distinguished between the personal data

processed on different devices and/or services, used concrete examples to illustrate the types of personal data processed as well as the different purposes they could serve, and offered different versions of the privacy/data policy depending on the interested audience. To justify the poorer notes, participants flagged, among others, the mixing of information relevant for different users in a single privacy/data policy, the confusion arising from the reference to multiple regulatory frameworks in the same document (*e.g.*, CCPA and GDPR), and the use of overly broad language when describing the purposes for which the personal data are processed.

Form

When it comes to transparency, the form is as important as the content. According to Article 12(1) GDPR, controllers must provide the information listed in Article 13 and 14 "in a concise, transparent, and intelligible" way, "using clear and plain language". This requires controllers to communicate in such a way as to avoid "information fatigue", and to ensure that the information "is understood by the average member of the intended audience".[49] Controllers must therefore identify the type of users whose data will be processed and adapt the tone and language of their policy accordingly. This is especially true when it comes to information provided to children.[50] The reference to "clear and plain language" calls on controllers to refrain from relying on complex sentences and language structures, but instead provide concrete and definitive information that is "not phrased in abstract or ambivalent terms or leave room for different interpretations".[51] Language qualifiers such as "may", "might", "some", "often" and "possible" should be avoided, as well as the use of "overly legalistic, technical or specialist language or terminology".[52] Transparency is therefore context-dependent. As a result, providers of particularly complex technologies, or those targeting less-literate groups, will need to put in the effort for their audience, and most notably, describe unambiguously the most important anticipated consequences the data operations hold for those involved.[53]

Article 12(1) GDPR also states that the information must be provided "in writing or by other means, including, where appropriate, by electronic means". The WP29 advocates for a layered approach, be it in a digital or non-digital context, to "allow website visitors to navigate particular aspects of the privacy notice that are of most interest to them".[54] This is one of the many ways

[49] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) paras 8–9.
[50] Article 12(1) GDPR. See also: ibid 14–16..
[51] ibid 12.
[52] ibid 13.
[53] ibid 10, which adds a new element to the list of Articles 13 and 14, namely "what the most important consequences of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject".
[54] ibid 17–19, 35–38.

to reconcile the requirements of conciseness and completeness.[55] If controllers decide to go for a layered privacy/data policy, the WP29 requires the first layer of information to always include a description of data subject's rights.[56] In the same vein, controllers must always proactively communicate any change in how data subjects can exercise their prerogatives under Article 15-22 GDPR.[57]

It is also crucial that controllers provide the information relating to the personal data processed, the processing purposes and the applicable lawful grounds in a meaningful way, *i.e.*, by pairing each personal data with one or more purposes, and each purpose with a single lawful ground.[58] Presenting that information separately by, for instance, listing the processing purposes in a dedicated section falls short of achieving the very goal of transparency, *i.e.*, allowing citizens to understand and, if necessary, challenge controllers' processing activities. Knowing the exact purpose that the controller intends to justify based on its legitimate interests under Article 6(1)f is, in that sense, an essential piece of information to corroborate – and eventually contest – the output of the corresponding balancing exercise. While we noted a significant increase in the amount of providers that did make an effort to link all (from 10% in 2020 to 56% in 2022) or some (from 74% and 45% in 2020 to 89% and 88% in 2022) of these pieces of information (fig. 5), the absence of any link between the personal data processed and the processing purposes, and between each processing purpose and the applicable lawful ground remains, in 2022, a reality for, respectively, 12% and 22% of controllers.[59]

Overall, participants rated the form of 57% (in 2020) and 66% (in 2022) of the privacy/data policies as "very satisfying" or "satisfying". Among the most often cited grievances, they flagged the absence of menu, table of content, or otherwise clear structure, as well as the length of some of the documents, with 13% exceeding 10,000 words in both 2020 and 2022 (fig. 6). The study also uncovered good practices, among which the use rich text such as bold and italic formatting, tables, boxes, and always-on navigation panels. In some cases, OSPs also used images, GIFs, and

[55] Inspiration can be taken from, among others, Nicolás E Díaz Ferreyra and others, 'Preventative Nudges: Introducing Risk Cues for Supporting Online Self-Disclosure Decisions' (2020) 11 Information 1; Arianna Rossi and Gabriele Lenzini, 'Transparency by Design in Data-Informed Research: A Collection of Information Design Patterns' (2020) 37 Computer Law & Security Review 1; Raúl Pardo and Daniel Le Métayer, 'Analysis of Privacy Policies to Enhance Informed Consent (Extended Version)' (INRIA Rhône-Alpes 2019) RR-9262 <https://hal.inria.fr/hal-02067924v2/document> accessed 4 January 2022.

[56] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) para 36.

[57] ibid 29.

[58] Ausloos, Mahieu and Veale (n 23) para 60 also advocate for such an approach, if by putting the emphasis on the need to provide tailored information *ex post*, *i.e.*, as part of an answer to an access request. Doing so also naturally follows from the very goal of transparency, itself linked to overarching principle of fairness.

[59] It is interesting to highlight that controllers seem to have more difficulties in linking the processing purposes with the corresponding lawful ground than the personal data with the processing purposes.

videos to complement textual descriptions to make it more accessible to a less qualified – or interested – audience, and even resorted to a touch of humour in the form of plays of words.

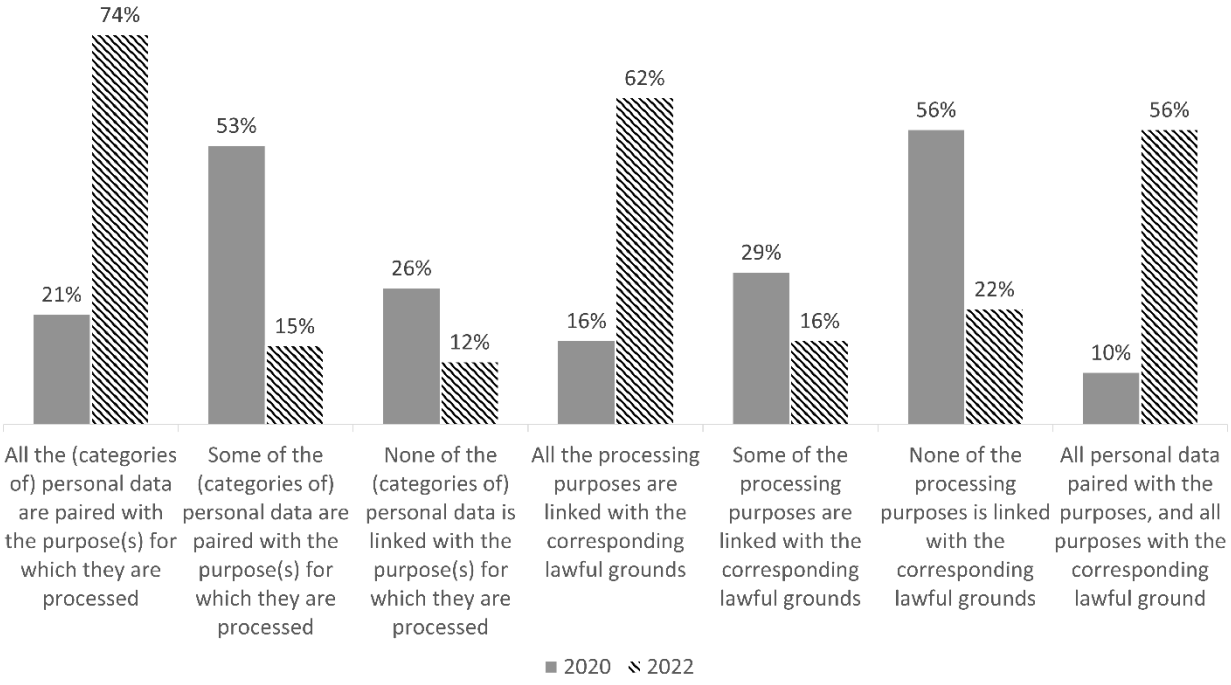

Figure 5 - Link personal data – purposes – lawful grounds in the privacy/data policy

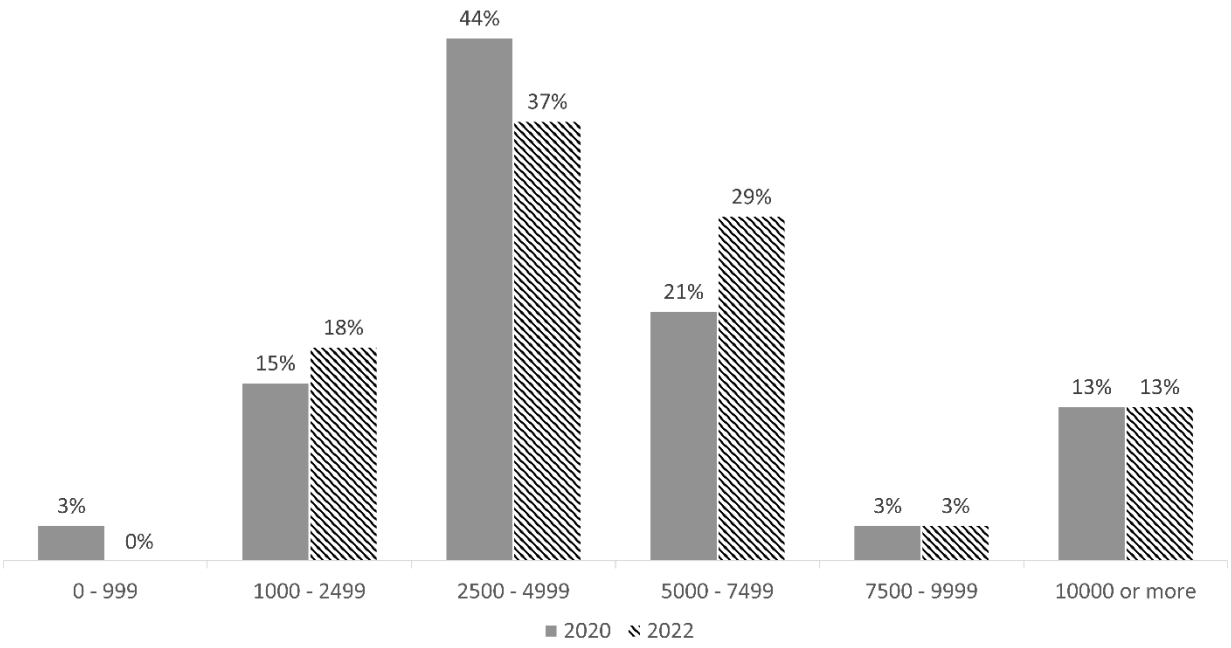

Figure 6 - Word count for the privacy/data policy

Filing the Access Request

Article 15 GDPR complements the ex-ante transparency requirements laid down in Articles 13 and 14 GDPR by granting data subjects the right to request (1) confirmation that personal data concerning them are being processed, (2) a copy of the personal data undergoing processing and (3) individualised details on the elements listed in Article 15(1)a-j and (2) GDPR. As such, it offers data subjects the possibility to go beyond the privacy/data policy and request more information on how their personal data are *actually* processed, offering an additional, individualised layer of transparency.[60] With the information gathered from OSPs' privacy/data policies, participants submitted access requests based on the template attached to the present paper, using the means specifically referenced by the controllers to that effect.

Form of the access request

Right from the get go, it is worth highlighting that 6% (in 2020) and 4% (in 2022) of OSPs still failed to mention how data subjects could exercise their rights, despite the obligation for controllers to "facilitate the exercise of data subject rights" in Article 12(2) and Recital 59 GDPR (fig. 7).[61] Email and contact form were, both in 2020 and 2022, the most popular means of communications proposed by controllers to exercise data subject's rights.[62] As pointed out by the EDPB in its Guidelines on the right of access, the GDPR "does not impose any requirement regarding the form of the request", nor any rule that the data subject "must observe when choosing a communication channel through which they enter into contact with the controller".[63] As a result, controllers are also expected to act upon requests that, even though submitted through a channel that is different from the one specifically indicated in the privacy/data policy, have nonetheless reached the correct addressee.[64] This would not be the case, if, for instance, the data subject sends their request to "a random of incorrect email or postal address", or when contacting "an employee

[60] For a detailed overview and analysis of all the information that needs to be shared in response to the exercise of a right of access, see: Laurens Naudts, Pierre Dewitte and Jef Ausloos, 'Meaningful Transparency through Data Rights: A Multidimensional Analysis' [2022] Research Handbook on EU Data Protection Law 530; Gabriela Zanfir-Fortuna, 'Article 15. Right of Access by the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020).

[61] Articles 13(2)b and 14(2)c only oblige controllers to mention the *existence* of data subject's rights; yet, the Working Party 29 is of the opinion that "this information should be specific to the processing scenario and include a summary of what the right involves and *how* the data subject can take steps to exercise it and any limitations on the right" (emphasis added). See Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) 39.

[62] Also corroborated by other empirical studies, as explained in: Habu and Henderson (n 7).

[63] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 52.

[64] ibid 53. As noted in ibid 57, such requests still trigger the one-month time limit of Article 12(3).

who may not be involved in the processing of requests concerning data subject's rights (*e.g.*, drivers, cleaning staff, etc.)".[65]

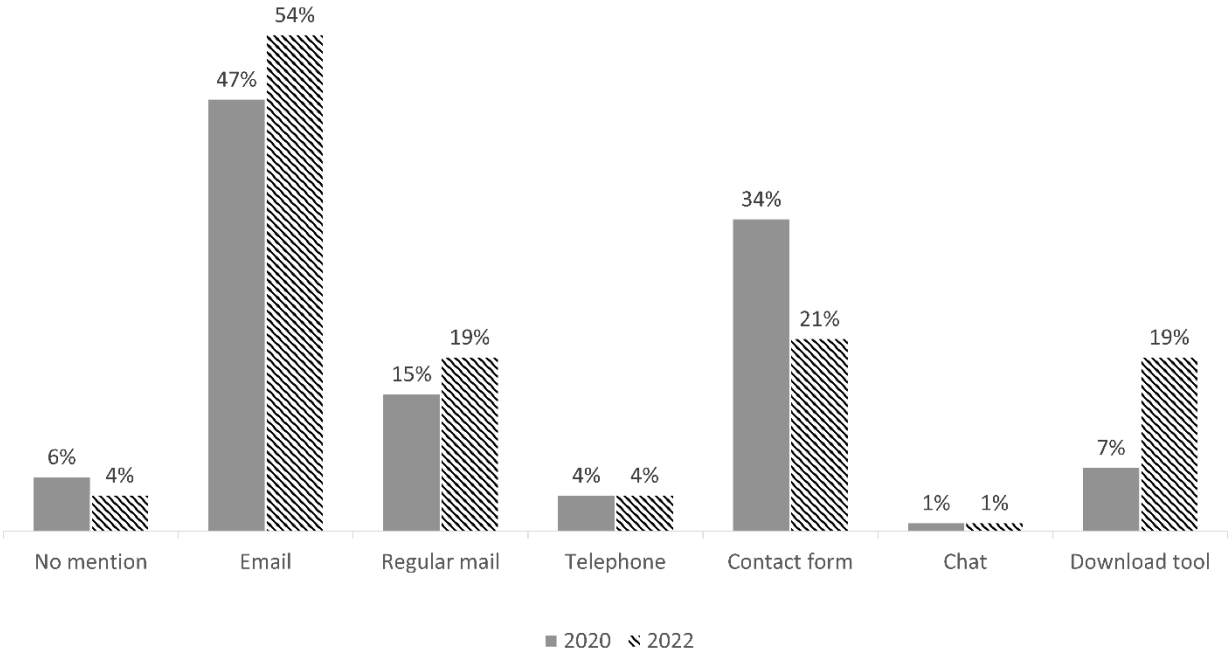

Figure 7 - Means mentioned in the privacy/data policy to request access

Besides, a substantial amount of OSPs (25% in 2020 and 28% in 2022) did not offer non-registered users the possibility to file an access request using the means specifically set up to that effect, mainly because the process required the use of a contact form or a tool that was only available after logging in. Doing so severely limits the personal scope of Article 15 GDPR by restricting its applicability to *users* rather than to *data subjects*. This is particularly problematic since one of the purposes of the right of access is, precisely, to allow data subjects to become aware of processing operations carried out by entities they do not know about – and *a fortiori* are not registered users of. The same is true for processing activities of controllers that are not consumer-facing, and therefore do not even allow data subjects to register or create an account.[66]

The satisfaction rate for the submission process remained stable in both studies, with 62% (in 2020) and 61% (in 2022) of participants who considered it either "very satisfying" or "satisfying". Still, 14% and 8% of participants expressed dissatisfaction, which they attributed to several factors

[65] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 54.
[66] This is the case, for instance, when a data subject exercises their right of access to obtain a copy of the personal data held by the many actors involved in programmatic advertising, such as supply-side platforms, ad exchanges and demand-side platforms. Or when they request access to personal data processed by public services. Although none of these types of controllers were included in the scope of the studies.

(fig. 8). Some reported that the dedicated contact form was only available after looking for it via Google Search or browsing forums such as Reddit. Others noted that, in the absence of data protection-specific contact point, the process of finding even a general-purpose email address was particularly tedious. During the 2020 study, one OSP only offered the possibility to get in touch via regular post, which is, once again, at odds with the obligation for controllers to facilitate the exercise of data subject's rights and the recommendation to "provide means for requests to be made electronically, especially where personal data are processed by electronic means" (Recital 59 GDPR) – which was the case here. Confronted with a controller who had delegated the submission and handling of data subject's rights to a specialised third-party provider, one participant also noted that, "even though it shows awareness and dedication, the amount of information required to use that portal is questionable".[67]

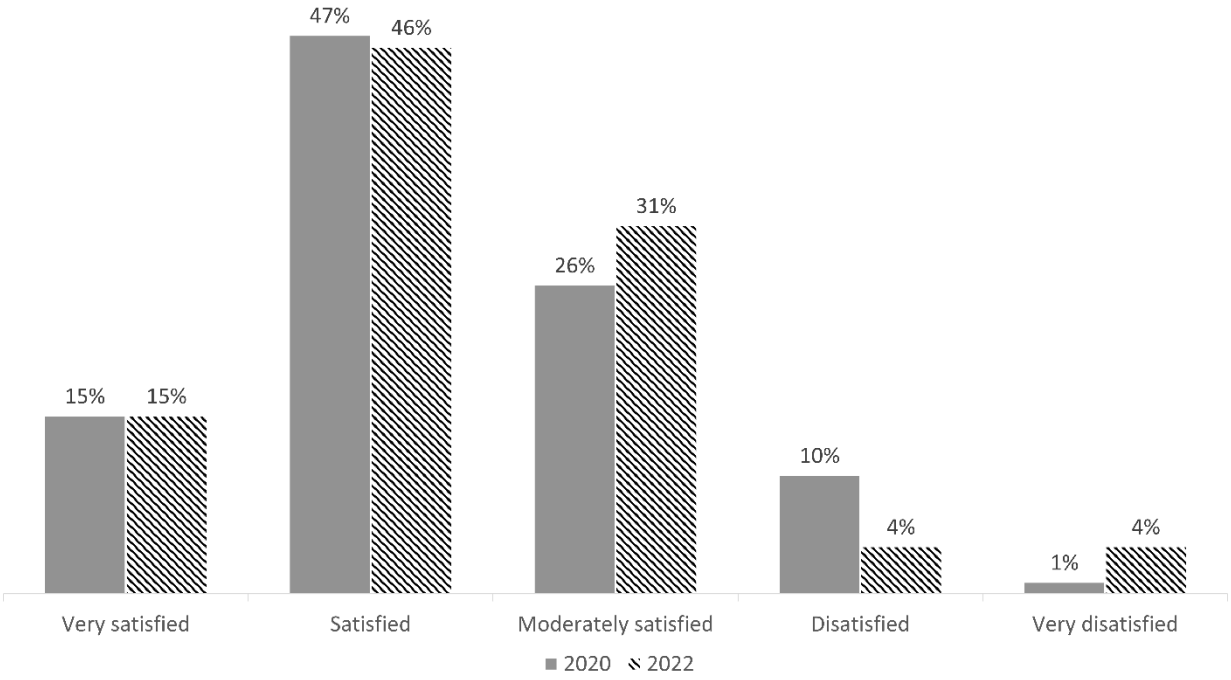

Figure 8 - Satisfaction rate for the privacy/data policy

Content of the access request

Beside the absence of formal requirements, the GDPR did not introduce substantive constraints for the exercise of data subject's rights either. In that sense, and as recalled by the EDPB, "it is sufficient for the requesting persons to specify that they want to know what personal data

[67] Plus, this paves the way for other issues such as the need for the controller to conclude a controller-processor agreement as per Article 28 GDPR, the risk of incompatible further processing by that third party for purposes other than handling access requests on behalf of the controller, the potential transfer of personal data to third countries, and the security risks associated with letting a third party directly access user data.

concerning them the controller processes", and the controller cannot refuse to act upon that request simply because the data subject failed to explicitly reference Article 15 GDPR.[68] This is a welcome clarification, as the right of access is meant to empower all individuals – including and especially non-lawyers – to grasp the existence of extent of processing activities involving their personal data. We could not, unfortunately, empirically evaluate controllers' leniency when faced with vaguely worded requests, as the template used to submit the initial request specifically mentions Article 15 GDPR. When confronted to such a situation, controllers are in any case expected to adopt a pragmatic approach and ask the data subject to clarify the subject matter and scope of their demand.

The EDPB also clarified that data subjects do not have to justify why they exercise their right of access, nor can controllers tailor or retain certain pieces of information depending on the objective they pursue by requesting access to their personal data. Advocate General Kokott paved the way for such an interpretation when stating that even though "Recital 41 [Directive 95/46] does indeed describe the purpose of access as being that the data subject may verify in particular the accuracy of the data and the lawfulness of the processing", the use of "in particular" in most language versions suggests that the purpose of the right of access goes further, "for even irrespective of rectification, erasure or blocking, data subjects generally have a legitimate interest in finding out what information about them is processed by the controller".[69]

This has also been confirmed more recently by Advocate General Nicholas Emilou, explaining that "the right of access the GDPR grants to data subjects is not conditional on their intention to use the data concerned for purposes relating to data protection, such as those set out in Recital 63 thereof".[70] Recital 63, he adds, "is rather meant to emphasise the significance, within the scheme of the GDPR, of the right of access". The CJEU later confirmed that reasoning, stating that "the data subject is not required to state the reasons for the request for access to data, the first sentence of recital 63 of the GDPR cannot be interpreted as meaning that that request must be rejected if it concerns an objective other than that of becoming aware of the processing of data and verifying the lawfulness of that processing."[71] In neither the 2020 nor the 2022 study did we encounter any controller who objected or expressed reservations to act upon our requests simply because we did not provide a specific justification; that might well have been the case should we have disclosed the existence of the study, that is.[72]

---

[68] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 50.
[69] Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017], Opinion of Advocate General Kokott, ECLI:EU:C:2017:582, para 39.
[70] Case C-307/22 *FT v DW* [2023], Opinion of Advocate General Emilou, ECLI:EU:C:2023:315, para 17.
[71] Case C-307/22 *FT v DW* (n 27), para 43.
[72] On that note, it is worth noting that the European Data Protection Board (n 2) para 190 seems to set a relatively high threshold for a request to be considered "excessive" within the meaning of Article 12(5) GDPR. This defuses

Interacting with Controllers

Not a single OSP provided a completely satisfactory answer right away in 2020 (fig. 9). Only a small subset (7%) did so in 2022. We therefore had to engage with controllers to try and complete the missing information, using either the follow-up template attached to the present paper, or an ad-hoc response when confronted to a genuine request for clarification from a controller processing large and diverse datasets. While the process of interacting with OSPs was significantly smoother than reported in earlier, similar studies, participants were still confronted, as discussed below, to various obstacles such as inaction, delays, confusion, rudeness, and suspicion.[73]

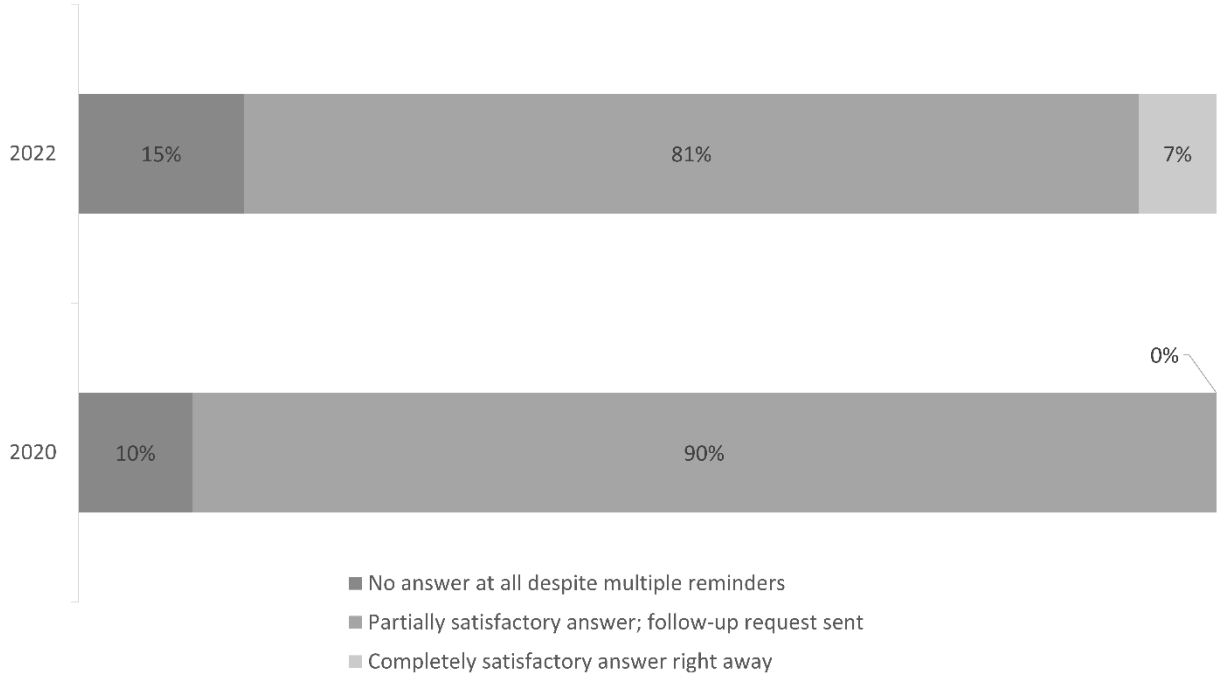

Figure 9 - Overview of the types of answers received

Reminders and success rate

In 20% (in 2020) and 16% (in 2022) of cases, it was necessary to send one or more reminders before obtaining a first substantive answer, *i.e.*, an answer that *actually* contained some or all information listed in Article 15 GDPR, regardless of its nature or form.[74] As logically recalled by

the potential argument that could be made as to the "excessiveness" of requests formulated in the context of academic research. Especially in the context of this empirical study, as we specifically avoided to “name and shame” so to not cause any “disruption”, to use the exact terms of the Board. Regardless, the study pursued a broader purpose than to “disrupt” controllers, which, in itself, is sufficient to discard that argument.

[73] See the conclusions drawn by the authors of the papers mentioned in (n 8).

[74] What we did not consider as first substantive answers included, for instance, requests for clarification, any form of verification of identity and replies redirecting us to another department.

the EDPB, a reminder is not to be interpreted as a new request, and therefore should not be taken into account when assessing whether a request is "excessive" within the meaning of Article 12(5) GDPR.[75] Still, 10% (in 2020) and 15% (in 2022) of OSPs did not provide any answer at all, despite multiple reminders (fig. 9).[76] Among those that did provide a partially satisfactory answer, 16% (in 2020) and 42% (in 2022) had provided all the missing elements at the end of the follow-up process, while 20% (in 2020) and 25% (in 2022) had complemented their initial response with more, but not all, the information required by Article 15 GDPR (fig. 10). One should note, however, a significant improvement between both studies, as 64% of OSPs stood by their first reply in 2020, compared to "only" 34% two years later. On average, it took participants 2.66 (in 2020) and 2.88 (in 2022) interactions to obtain a final answer, *i.e.*, either a fully satisfactory answer or the last answer obtained before the closing of the legal-empirical study.

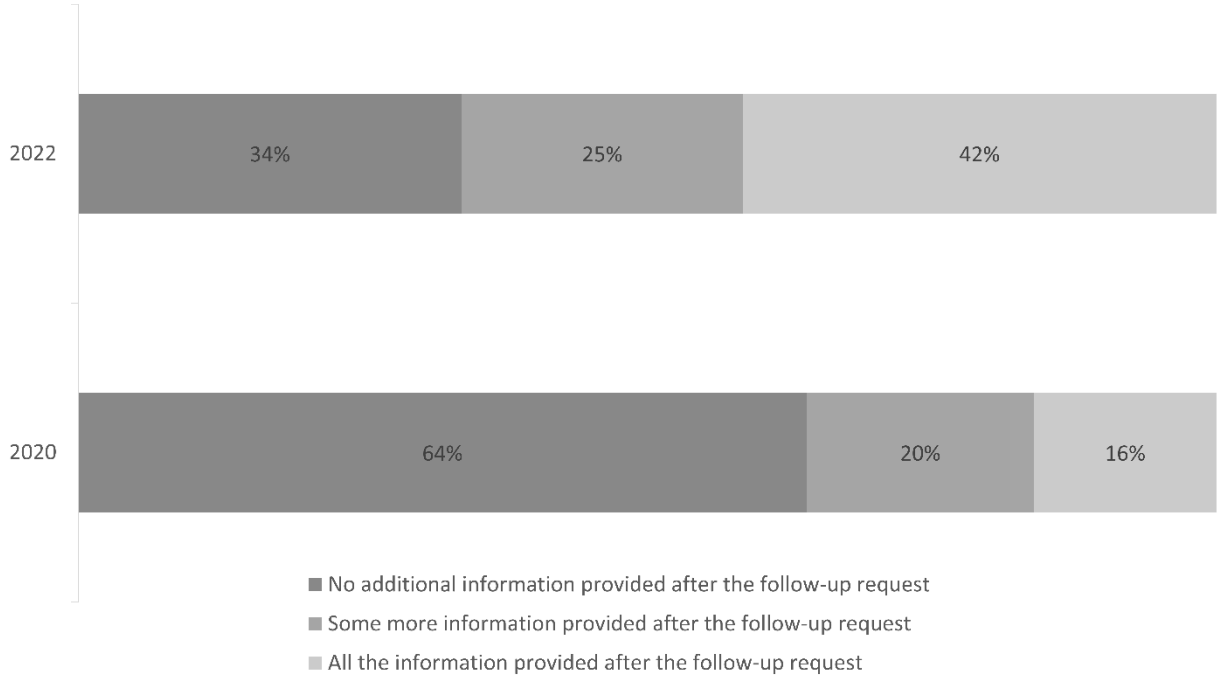

Figure 10 - For the OSPs that only provided a partial answer, amount of additional information obtained at the end of the follow-up process

[75] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 29.
[76] The reminder policy for the legal-empirical study was the following: (i) if participants did not receive an acknowledgment of receipt, they sent a reminder 1 week after the initial request; (ii) if participants received an acknowledgment of receipt: (a) with a clear time indicator (*e.g.*, 'within 10 days', 'before the end of this week'), they sent a reminder immediately after that time had passed; (b) with an approximate time indicator (*e.g.*, 'within a reasonable time frame', 'as soon as possible', 'shorty', 'within the days'), they sent a reminder 2 weeks after the initial request; (c) with no time indicator whatsoever, they sent a reminder 1 week after the initial request.

Request for specification

As a rule, data subjects are entitled to obtain full disclosure of all data relating to them. Upon reception of the broad initial request, however, some OSPs asked data subjects to specify their demand by identifying the exact pieces of information they would like to obtain. Such a limitation of the right of access, states the EDPB, can only be justified in three scenarios, namely (i) when the data subject themselves have limited the scope of their request, (ii) when the controller processes a large quantity of data over several branches of activity and therefore has reasonable doubts that a request formulated in general terms really aims at receiving the entirety of the personal data or (iii) when specific exceptions or restrictions apply (see below).[77]

Regardless of whether the quantity and diversity of the personal data processed by these OSPs were large enough to justify a request for specification, none of them did, in fact, accompany that request with "a clear overview of all processing operations that could concern the data subject, including especially those that the data subject might not have expected", nor informed them on "how to get access to the remaining parts of the processed data".[78] That information, however, is necessary for data subjects to make an informed decision as to whether they really wish to obtain *all* the information listed in Article 15, from *all* branches and sectors. Confronted to a request for specification, data subjects can simply confirm their intention to get a full picture, which participants systematically did in both studies. Two of them, however, felt that this was a strategy deployed by the respective OSPs to delay the process or hide certain aspects of their processing, as they only provided limited information in their first reply and asked them to pinpoint the missing bits, effectively shifting the burden of identifying the relevant processing activities onto data subjects.

Identification and authentication

To answer an access request, controllers must both *identify* the personal data relating to the data subject, and *authenticate* their identity to confirm that they are actually entitled to received that information.[79] This is rather straightforward when the request concerns information relating to an *identified* individual; say, when a registered customer of an e-commerce platform exercises their right of access to obtain information about their order history. If that request is filed directly through the platform, or using the email address used to register, the controller can easily single

[77] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) paras 35, respectively points a), b) and c). See also Recital 63, which states that "[w]here the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates"

[78] As mandated by ibid 35, b), right before and after example 5.

[79] Acting on a request formulated according to Article 15-22 GDPR indeed requires the identification of the data subject, as a right only exists insofar as it is granted to a specific person, and that person exercises it.

out the relevant datasets and confirm the identity of the data subject since the above-mentioned information is typically linked to a specific account.

When the request concerns information relating to an *identifiable* individual, however, the controller might not always possess information necessary to identify the data subject and retrieve the relevant personal data.[80] This is notably the case when, as foreseen in Article 11(1) GDPR, the controller has refrained from collecting, pseudonymised or deleted the identifying reference.[81] If the controller is able to demonstrate that it is not or no longer in position to identify the data subject directly, and, if possible,[82] informs them of that impossibility, Article 11(2) GDPR exempts it from complying with Articles 15-20, while Article 12(2) allows it to refuse to act on requests formulated according to Articles 15-22.[83] In such cases, Article 11(2) GDPR nonetheless allows data subjects to provide additional information enabling their identification, therefore compelling controllers to act upon their request.[84]

Article 12(6) GDPR also allows controllers, where they have "reasonable doubts concerning the identity of the natural personal making the request" to "request the provision of additional

[80] As indeed clarified by the Recital 26, the identifiability test used to assess whether a piece of information qualifies as personal data should take into account "all the means reasonably likely to be used, such as singling out, either by the controller *or by another person* to identify the natural person directly or indirectly" (emphasis added). In turn, this means that the controller itself does not always have the information needed to reidentify the data subject making the request. See also, on that point: Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' 15–17 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 16 January 2023.

[81] In that sense, Article 11(1) is a specific manifestation of the principle of data minimisation enshrined in Article 5(1)c. It should also be pointed out that Article 11(1) only applies to situations where the controller process personal data that does not or no longer relate to an *identified* natural person, but still relate to an identifiable individual (*e.g.*, when the controller has pseudonymised the personal data at stake), since the GDPR simply does not apply to properly anonymised data.

[82] The "if possible" suggests that the provision of such information to data subjects is not a strict condition for the applicability of the exemption of Article 11(2).

[83] There is a notable difference between Articles 11(2) and 12(2). The former is an exemption to comply with Articles 15-20, while the scope of the latter also extends to Articles 21-22. In any case, controllers should also inform the data subject of the nature of the additional information required to reidentify them for the purpose of exercising their right. See European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 68.

[84] See Recital 57 and ibid 60–61. Example 11 of the Guidelines is, in that sense, particularly enlightening. According to the Board, a data subject has the possibility, for instance, to provide the controller with the cookie identifier stored in their terminal equipment to request information about the personal data collected and processed by a specific third-party tracker embedded on the controller's website, therefore circumventing the initial impossibility for the controller to identify the relevant set of processing operations. This should even be done automatically when the data subject exercises their right directly through the website, as "a link between the data processed and the data subject can be found". However, while many controllers have developed excellent identifying infrastructures for, say, the purpose of providing analytics or targeted advertising, they are currently only "encouraged" to build similar systems to easily identify and authenticate data subjects for the purpose of letting them exercise their rights under the GDPR. See: ibid 68. See also, on that issue: Ausloos, Mahieu and Veale (n 58) paras 124–126.

information necessary to confirm the[ir] identity", which 18% and 28% of OSPs used, respectively, in 2020 and 2022. "As a rule", states the EDPB, "the controller cannot request more personal data than is necessary to enable this authentication", and should preferably use authentication methods that are already in place, such as using the same credentials used by the data subjects to log-in on the service, or relying on multi-factor authentication if enabled to secure access to the platform.[85] These two methods were, by far, the most popular solutions deployed by controllers to verify the identity of data subjects, and were used by 28% (in 2020) and 36% (in 2022) of OSPs. In any case, controllers "shall carry out a proportionality assessment, which must take into account the type of personal data being processed, the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure".[86] In light of the above, the EDPB considers that asking for a copy of an identity document is generally disproportionate if any of the above-mentioned authentication methods can be used.[87] Yet, 7% (in 2020) and 3% (in 2022) of OSPs explicitly requested participants to provide a scan of their ID card.

Limitations and restrictions

Article 15(4) GDPR limits the right to obtain a copy of the personal data undergoing processing – if not the right to obtain confirmation of the processing as well as the information listed in Article 15(1) and (2) – insofar as its exercise "adversely affect[s] the rights and freedoms of others". Conflicting rights, illustrates Recital 63, include "trade secrets or intellectual property and in particular the copyright protecting the software", but should not, in any case, lead to "a refusal to provide all information to the data subject".[88] Controllers that rely on Article 15(4) GDPR to refuse to act on an access request must inform data subjects, without undue delay, of the reasons justifying their decision so to allow them to consider an action against the refusal.[89] None of the OSPs investigated in 2020 and 2022 invoked that limitation. Same goes for the possibility to refuse to act on, or charge a reasonable fee, when confronted to a manifestly unfounded or excessive request stemming from Article 12(5) GDPR. Which is to be welcomed, as some providers might have been tempted – wrongfully so – to hide behind the "excessiveness" of the requests submitted by some participants who dug quite deep into specific aspects of their processing

[85] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) paras 65, 66, 72, 73, more specifically example 13. See also, on that same idea: Article 29 Working Party, 'Guidelines on the Right to Data Portability' 14 <https://ec.europa.eu/newsroom/article29/items/611233> accessed 12 May 2023.
[86] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 70.
[87] ibid 73. The circumstances under which requesting an ID would be proportional are listed in ibid 78–79.
[88] The Board details the three steps of the balancing exercise between the fundamental right to data protection and other conflicting rights and freedoms in European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 173. More specifically, see examples 35 and 36.
[89] ibid 174.

activities.[90] As indeed recalled by the EDPB, "the complexity of data processing [can] not be used as an argument to limit the access to all data".[91]

Article 23(1) GDPR also paves the way for Member States to "restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 [...] when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard" one of the ten objectives listed in points (a) to (j). The EDPB has clarified that such restrictions ought to be interpreted narrowly,[92] and the CJEU explained they cannot undermine the rights conferred by the Charter.[93] When relying on such a national provision, controllers are expected to both demonstrate how the corresponding legislation applies to them, and proactively inform data subjects that they are – or intend to – invoke that restriction.[94] Exactly as for Articles 15(4) and 12(5), none of the OSPs investigated in 2020 and 2022 referred to national law to stall or refuse to act on our access requests. The decision in case C-307/22 is particularly interesting in that regard. In his conclusions, Advocate General Nicholas Emilou indeed interpreted Article 23(1)I GDPR as allowing Member State to maintain or enact national legislation that would require patients to reimburse the costs incurred by doctors in retrieving and providing the personal data contained in medical records, "provided that the restriction to the right of access is, in the light of all relevant circumstances, necessary and proportionate to the objectives of protecting public health and the doctors' freedom to conduct a business".[95] The Court unequivocally diverged from the above and clarified that that provision "does not permit the adoption of a piece of national legislation which, with a

[90] As suggested by the use of "in particular" in Article 12(5), the "repetitive" nature of the request is only one of the factors that could make a request "excessive". Besides, multiple requests emanating from the same data subject should not always be considered as "repetitive" within the meaning of that provision. First, and as can be inferred from the wording of Article 15(3) ("for any *further* copies"), data subjects can ask more than one copy – if paid for – , so that a second identical request should not automatically be considered as "excessive". Second, data subjects can also formulate new requests – *i.e.*, requests that differ either in scope or intervenes at a later point in time, when the processing at stake might have evolved –, requests for clarifications, and reminders. These, while they might partially overlap with an earlier request, should not be considered "excessive". This is also pointed out in: Ausloos, Mahieu and Veale (n 58) para 111.

[91] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 141.

[92] European Data Protection Board, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' (n 16) para 3.

[93] Joined Cases C-511/18, C-512/18, C-520/18 (n 17) para 210. On that note, It is worth reiterating that the right of access is an explicit part of the fundamental right of protection of personal data (Article 8(2)).

[94] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) para 68.

[95] Opinion of Advocate General Emilou in Case C-307/22 (n 73), para 71. It is worth noting the circumstances in which that led the Advocate General to reach such a conclusion, namely the fact that the national legislation at stake only restricted *one form of access* (*i.e.*, the right to obtain a copy, not the other components of Article 15), only by *making it conditional* upon the payment, by data subjects, of the costs incurred by the controllers. See ibid 37. The risk of leaning towards an overly broad interpretation of the possibility offered by Article 23 is, therefore, rather limited.

view to protecting the economic interests of the controller, makes the data subject bear the costs of a first copy of his or her personal data undergoing processing".[96]

Other obstacles faced along the way

Overall, the satisfaction rate for the follow-up process improved between 2020 and 2022, going from respectively 28% to 42% of participants being either "satisfied" or "very satisfied" (fig. 11). That said, the study nonetheless unearthed several issues. One participant noted that four reminders were necessary to get the OSP to react to their initial request. Another received a broken URL to download the copy prepared by the controller. Many participants, in both iterations of the study, had their "ticket" automatically closed right after receiving the first substantive answer from the OSP, with no possibility to follow-up on it other than opening a new one. Doing so, underlined a participant, ran the risk of the controller considering that second request as a request for a "further copy" within the meaning of Article 15(3) GDPR, for which the OSP could potentially charge a "reasonable fee".[97] Regardless, arbitrarily marking a request as completed drastically complicates the exercise of the right of access, as contesting the answer, requesting additional elements or asking for clarifications requires data subjects to start again from scratch.

Other participants regretted that the first contact they had was with the customer service rather than with the privacy and data protection team, which required the former to first forward the request to the competent department. In one case, the person responsible for dealing with access requests was on holiday, which delayed the process by a week. Building, once again, on the obligation for controllers to "facilitate the exercise of data subject's rights", the EDPB recommends the implementation of "autoresponder systems to inform of staff absences and appropriate alternate contact and, where possible, mechanisms to improve internal communication between employees on requests received by those who may not be competent to deal with such requests". This is all in controllers' best interest, as internal communication and organisational issues do not suspend the one-month time limit (see below).

One participant of the 2020 study qualified the interaction process as "quite chaotic", as the access request led to their account being suspended without prior notice. To restore the said account, the participant had to go through multiple steps involving both the legal and customer support desks. An access request should, obviously, not lead to any such side effects, as recalled by the EDPB when stating that "the controller shall not deliberately escape the obligation to provide the requested personal data by erasing or modifying personal data in response to a

[96] Case C-307/22 (n 27) para 69.

[97] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 29. As hinted at in (n 81), it is essential to distinguish requests for further copies (*i.e.*, same scope, short timeframe), from new requests, and request for clarifications.

request for access".[98] Brought to light in earlier studies,[99] we only encountered bad faith and irritation from one single OSP in 2020, who insisted that we justified why we were looking to get access to our personal data even though we "fully understood the nature of the service". Yet it's not all doom and gloom, as some participants also experienced responsiveness, good faith, friendliness, and attention to details on their journey to access. One OSP even called to explain that it had never been confronted to such a request, but nonetheless wanted as much information as possible to get the legal and software development teams to prepare a complete response. This is in line with the EDPB recommendation to clear any reasonable doubt directly with the data subject.[100] That provider also provided regular updates on the process, even though we did not specifically ask to be kept informed.

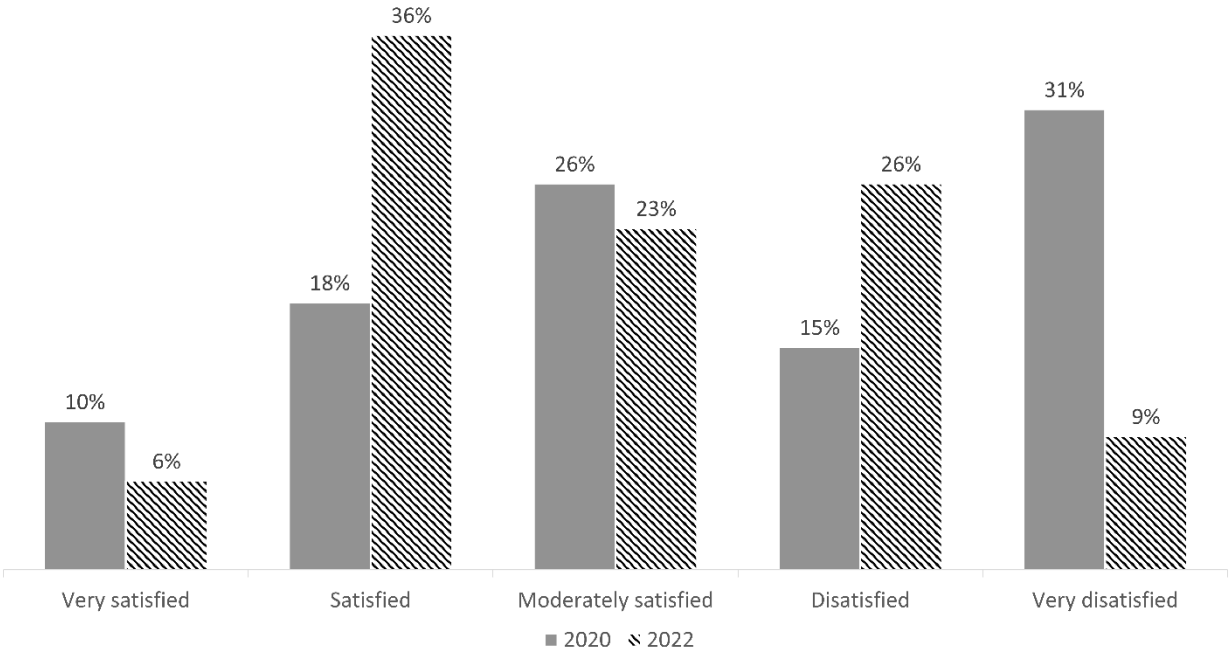

Figure 11 - Satisfaction rate for the follow-up process

Assessing the Final Answer

In general, the satisfaction rate for the final answer substantially increased in 2022, with 55% of participants being either "satisfied" or "very satisfied" of what they had obtained from OSPs before the closing of the legal-empirical study, compared to 33% in 2020 (fig. 12). That being said,

[98] ibid 39.
[99] As noted in Ausloos and Dewitte (n 6) 11–12, for instance.
[100] As noted by the European Data Protection Board (n 14) para 50, "in case of any doubts it is recommended for the controller to ask the data subject making the request to specify the subject matter of the request".

we encountered both substantial and formal issues with some OSPs' answers, as well as delays when trying to complete the generic information usually provided spontaneously.

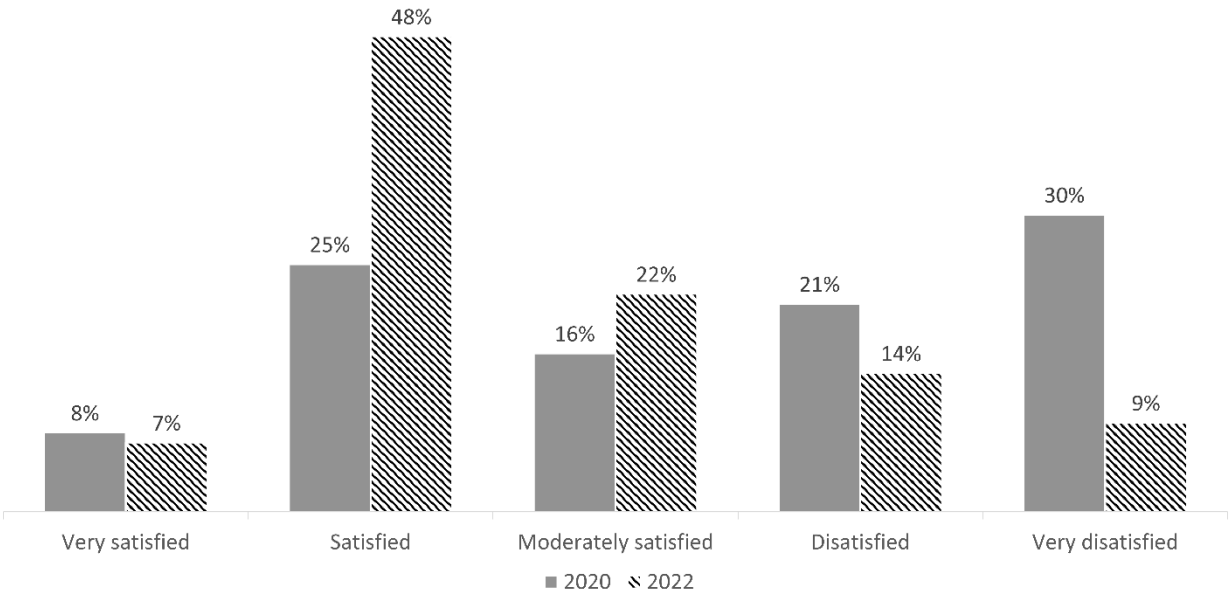

Figure 12 - Satisfaction rate for the final answer

Timing and delays

According to Article 12(3) GDPR, controllers must answer access requests "without undue delay and in any event within one month of the receipt of the request".[101] As recalled by the EDPB, this means that, where possible, controllers should strive to provide the requested information as soon as possible; the one-month time limit is, in that sense, a ceiling rather than a target.[102] The clock starts ticking, adds the Board, "when the request reaches the controller through one of its official channels", and regardless of whether the controller is, in fact, aware of the request.[103] Written acknowledgment of receipt is, if not a mandatory procedural requirement, considered as good practice.[104] That one-month time limit, stipulates Article 12(3) GDPR, may be extended by two further months depending on the complexity and number of the requests.[105] None of the

[101] That one-month time limit, states ibid 160, should be calculated in accordance with Regulation 1182/71.
[102] ibid 158.
[103] ibid 57, 159.
[104] ibid 57.
[105] According to ibid 163, some of the factors that could make a request complex include, for instance, "the amount of data processed by the controller, how the information is stored, especially when it is difficult to retrieve the information, for example when data are processed by different units of the organisation, the need to redact

OSPs investigated in 2020 and 2022 asked for such an extension – which is not to say that they all provided a final response on time.

Two scenarios warrant a suspension of the time limit. First, when a controller has reasonable doubts concerning the identity of the natural personal making the request and asks proceeds, as foreseen in Article 12(6) GDPR, to the necessary verification, provided that it does so without undue delay.[106] Second, when a controller that genuinely processes a large quantity of personal data is confronted to an access request formulated in broad terms and asks the data subject to specify their request.[107] It is worth pointing that neither of these two grounds for suspension should be used by controllers as delaying tactics by, for instance, systematically verifying the identify of data subjects in the absence of "reasonable doubts", or delaying the request for additional information or clarifications. Since no such suspension is foreseen for internal delay factors, such as the need to forward the request to the competent department or to retrieve the personal data from the relevant IT systems, it is in controllers' best interest to implement appropriate technical and organisational measures to deal with access requests as efficiently as possible. Repeated breaches of the time limit are, in that sense, a clear indication that the measures in place might not be suitable to the scope and/or complexity of the controller's processing activities.[108]

A relative majority of controllers, both in 2020 and 2022, provided a final answer within two months (fig. 13). When also considering the OSPs that took even longer to act on our requests, the study reveals that 51% (in 2020) and 77% (in 2022) of controllers failed to comply with the one-month time limit of Article 12(3) GDPR. While such finding is certainly symptomatic of deficiencies in the way controllers handle access requests, it deserves to be nuanced since participants did not keep track of genuine suspension causes, *i.e.*, when OSPs performed the necessary identity verification or requested clarifications in case of large-scale processing.[109] Still, 36% (in 2020) and 50% (in 2022) of controllers took more than a week to provide a first substantive answer, which suggests that the requirement to get back to data subjects "without undue delay" might not have been met (fig. 14).

information when an exemption applies, for example information regarding other data subjects or that constitutes trade secrets, and when the information requires further work in order to be intelligible".

[106] ibid 159. Controllers cannot therefore stall the procedure by leveraging the possibility to verify the identity of the data subject as a delaying tactic. Such behaviour could include, for instance, (i) systematically asking to verify the identity of the requesting party in case of absence of "reasonable doubt" or (ii) waiting before asking the data subject to provide the additional information to verify their identity.

[107] ibid 159 *juncto* 35.

[108] ibid 162.

[109] This is one of the weaknesses of the legal-empirical study, that could be improved in future iterations.

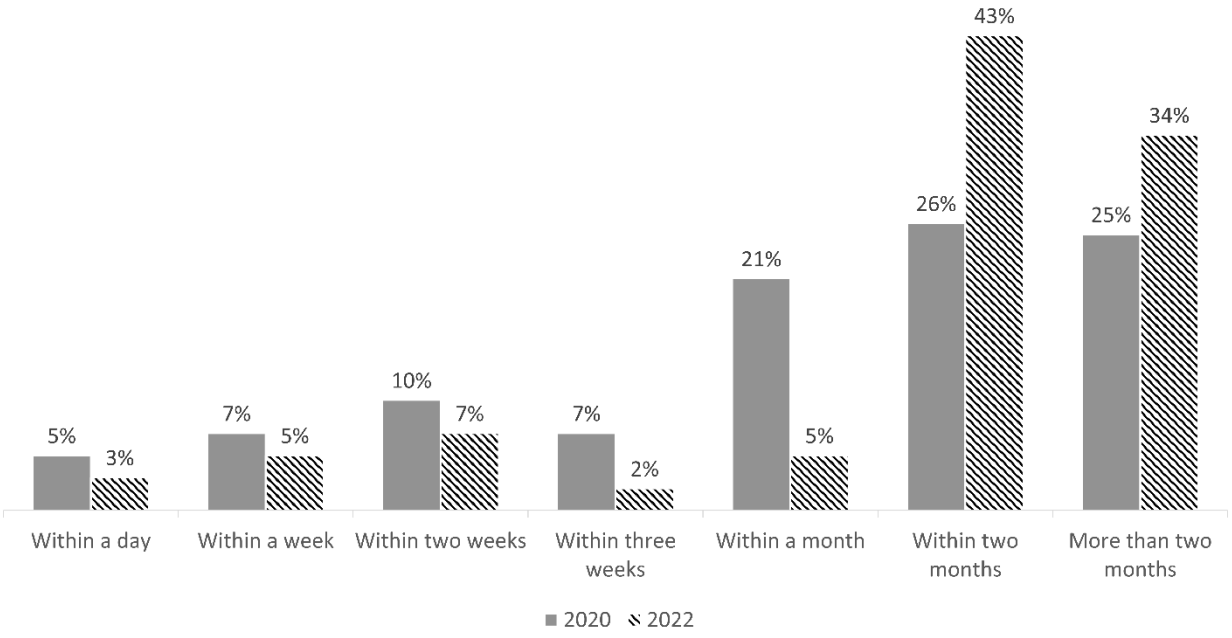

Figure 13 - Days between the initial request and the final answer

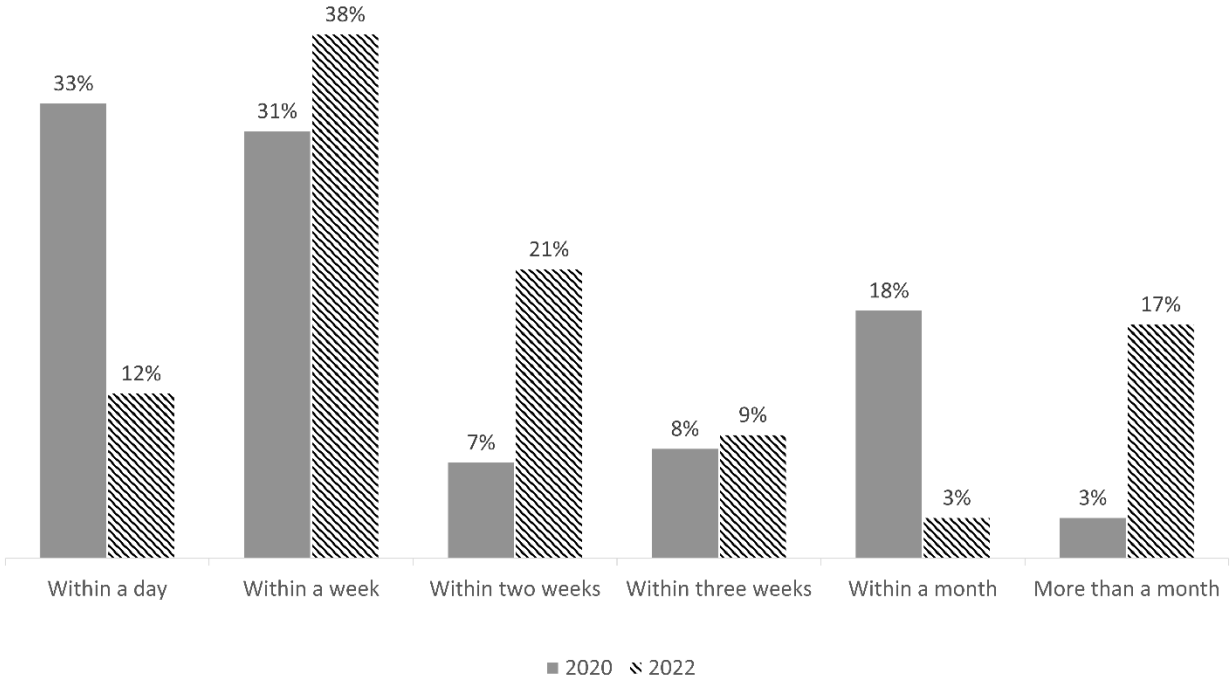

Figure 14 - Days between the initial request and the first substantive answer

Scope of the right of access–content of the answer

When comparing the information OSPs provided in their first substantive answer (fig. 15, 16) with what they shared in their final reply (fig. 17, 18), one can draw mixed conclusions.[110] On the one hand, OSPs scored better on all fronts in 2022 – if for a 2% drop concerning the copy of the personal data undergoing processing in their final answer. The average amount of information that OSPs did provide in, respectively, their first and last reply indeed jumped from 33% and 54% in 2020, to 69% and 81% two years later. On the other, the difference between the amount and quality of information participants received *after* engaging with controllers (Δ = +21% in 2020, and +12% in 2022) suggests, as noted in earlier studies, that data subjects must be proactive and show a certain degree of dedication to obtain all the details listed in Article 15(1) and (2) GDPR.[111]

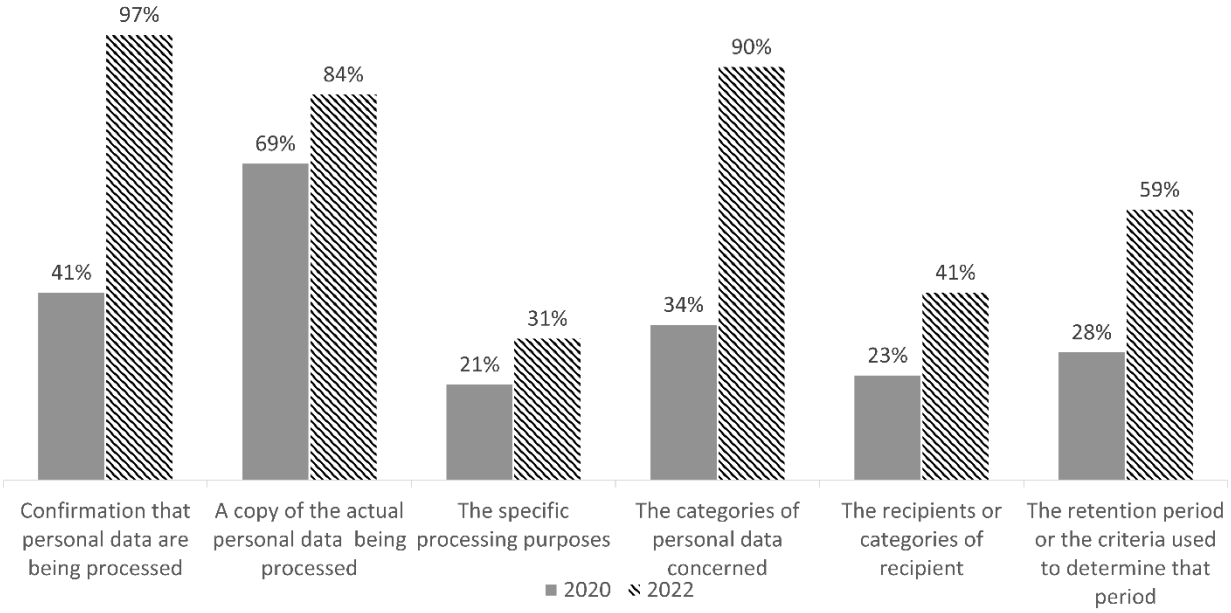

Figure 15 - Information provided in the first substantive answer (1)

[110] It should also be noted that, although the European Data Protection Board (n 14) para 114 recommends controllers to include information as to the applicable lawful grounds, that information was also left out of Figures 15, 16, 17 and 18 since it is not specifically included in the list of Article 15(1) GDPR.
[111] See in this regard also: Habu and Henderson (n 7).

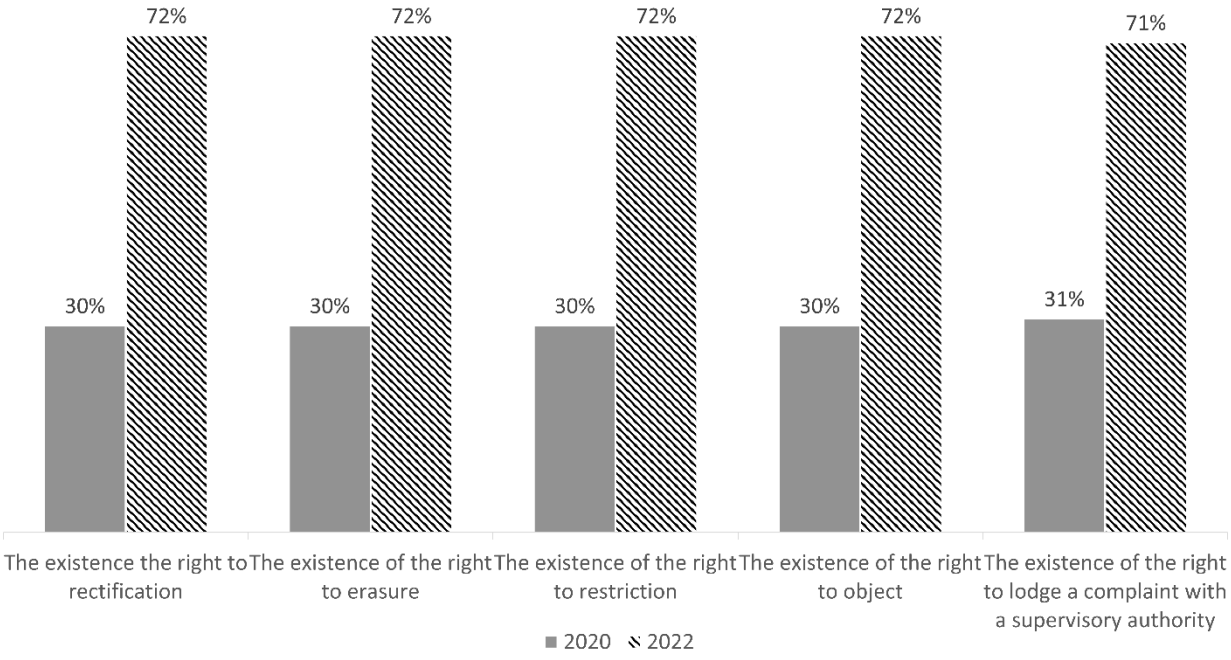

Figure 16- Information provided in the first substantive answer (2)

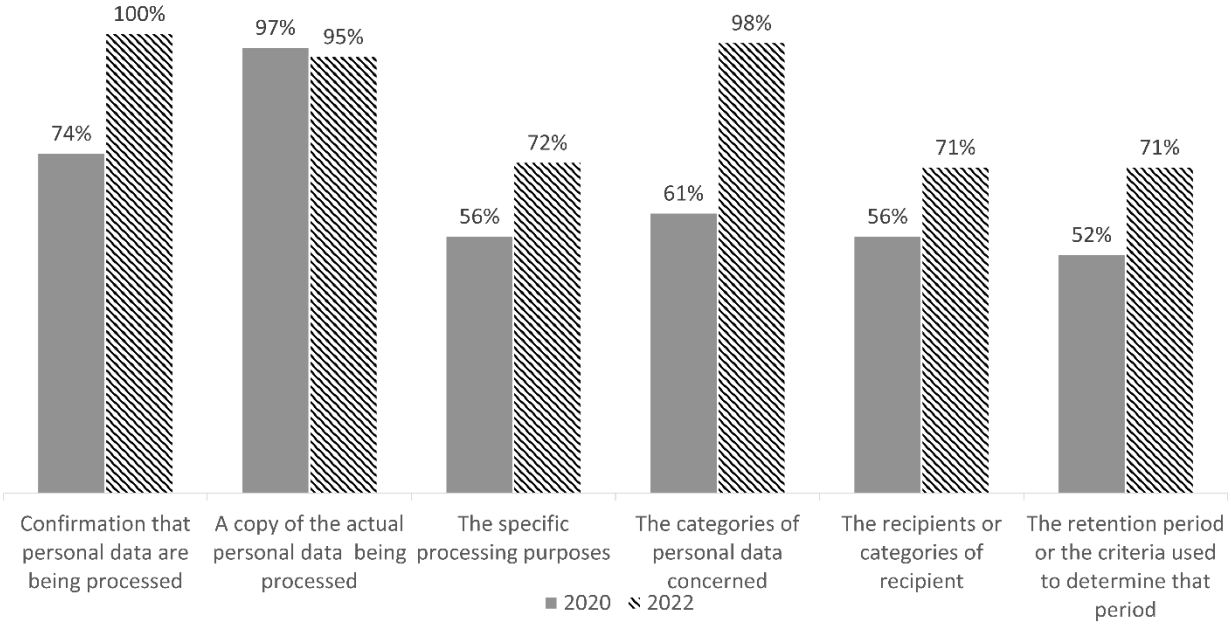

Figure 17 - Information provided in the final answer (1)

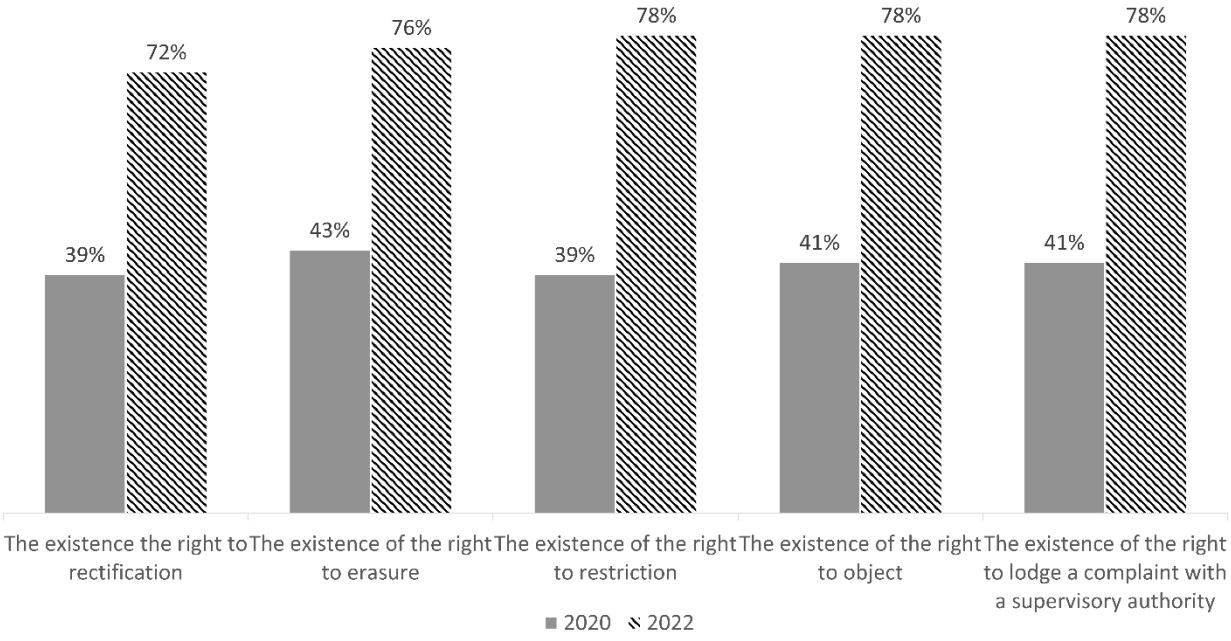

Figure 18 - Information provided in the final answer (2)

Our study reveals that, when confronted to a broadly formulated access request, controllers typically fail to provide data subjects with the specific processing purposes, the categories of personal data processed – at least in 2020 –, the retention period or criteria and the recipients or categories of recipient to whom the personal data have been transferred (fig. 15). These are also the pieces of information that are often missing from OSPs' final reply (fig. 17). When we asked to provide more details on these aspects, most OSPs redirected us to their privacy/data policy, or simply copy pasted the information already contained in that document.[112] While, as recalled by the EDPB, "carefully us[ing] text modules of their privacy policies" is not problematic *per se*, controllers must ensure that the information they provide data subjects is both "updated and tailored" to their particular situation.[113] This is crucial for information that is specific to the individual making the request, or is likely to evolve over time. In short, all the elements listed above. When acting on access requests, controllers must therefore avoid parroting their privacy/data policy, but instead detail the *actual* categories personal data undergoing processing, the *exact* purpose(s) for which they are processed, the *specific* – and, ideally, *named* –[114]

[112] Participants experienced such behaviour even when specifically requesting the OSPs not to simply provide a copy-paste of the privacy/data policy. That issue is also highlighted in Ausloos, Mahieu and Veale (n 58) para 58.
[113] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 113.
[114] Yet, it is worth pointing out that the CJEU recently confirmed that "the employees of the controller cannot be regarded as being 'recipients', within the meaning of Article 15(1)(c) of the GDPR", with the result that a data subject cannot rely on that provision to request a controller to disclose the identity of the employees who carried out certain processing operations A controller might be obliged to provide that information, however, when it "is

recipients to whom the data have been disclosed as well as information that is *precise* enough to allow data subjects to determine how long *their* personal data will continue to be stored.[115]

As noted by the EDPB, observed, derived and inferred personal data such as activity logs, attribute-based classifications and credit scores also fall under the scope of Article 15 GDPR.[116] As a result, controllers cannot limit their answer to a copy of the personal data *directly* provided by data subjects.[117] Yet, when enquiring about the processing of the personal data contained in bid requests for the purpose of serving targeted advertising, some participants noted that OSPs were unable – or, arguably, reluctant – to detail the actual data points collected by third parties to select the most relevant ads, and to provide more details on the functioning and outcome of the bidding process.[118] Besides, and while our study seems to indicate a relatively high compliance rate with the obligation to inform data subjects about their rights (fig. 16, 18), one should note that the survey did not account for the granularity of that information. Indeed, these rights vary depending on the lawful ground used to legitimise the processing at stake and should therefore also be tailored to the individual making the request.[119] This requires controllers, for instance, to identify the processing operations for which data subjects can request erasure, as well as the available grounds they can rely on to do so.[120]

Some participants noted that OSPs did not always include, at least in their initial reply, the copy of the personal data undergoing processing, which, according to the EDPB, should be regarded as the main modality for providing access rather than an additional right.[121] In other cases, OSPs

essential in order to enable the data subject to effectively exercise the rights conferred on him or her by that regulation and provided that the rights and freedoms of those employees are taken into account", which calls for a careful balancing exercise. See, on the above-mentioned points, Case C-579-21 J.M., *Apulaistietosuojavaltuutettu, Pankki S* [2023] ECLI:EU:C:2023:501, paras 73, 80, 83.

[115] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para respectively 115, 114, 116-117 and 118.

[116] ibid 97.

[117] As is the case when answering a request for portability according to Article 20. See, on that note, ibid 99.

[118] Of particular relevance in that context are the questions raised by the referring Court in the pending request for preliminary ruling in case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit*. The contested decision 21/2022 from the Gegevenbeschermingsautoritiet, the Belgian DPA, concluded that publishers and third parties such as Supply-Side Platforms (SSPs), Ad Exchanges (AdEx) and Demand-Side Platforms (DSPs) qualified as joint controllers for the processing of the information contained in bid requests. See: Gegevensbeschermingsautoriteit, Decision on the merits 21/2022 of 2 February 2022 in DOS-2019-01377 <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf> more specifically paras 362-402. Should the CJEU uphold that reasoning, and as noted in Article 26(3) GDPR, data subjects could send a request for access to any of the above-mentioned third parties.

[119] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 119.

[120] As was done for the right to erasure in: Ausloos, Mahieu and Veale (n 58) paras 70–74. Controllers should adopt the same approach for all the rights listed in Chapter III GDPR.

[121] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 23. The CJEU confirmed that in Case C-487/21 *FF v Österreichische Datenschutzbehörde* (n 25) para 32. That modality is

neglected the information listed in Article 15(1) and (2) and only provided that copy. The scope and form of that "copy", however, have been debated. In its Joined Cases C-141/12 and C-372/12, the CJEU stated that "it is sufficient for the applicant for a residence permit to be provided with a *full summary* of all [the personal data contained in the minute] in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive" (emphasis added).[122] Nearly ten years later, the Court fine-tuned its jurisprudence in Case C-487/21 by interpreting the notion of "copy" in light of the overarching principle of "transparency",[123] and ruled that the right to obtain a copy implies that "the data subject must be given a faithful and intelligible reproduction of all those data"; achieving that standard of intelligibility, added the Court, might require controllers to provide "copies of *extracts from documents* or even *entire documents or extracts from databases*", but only if doing so "is essential in order to enable the data subject to exercise effectively the rights conferred on him or her" (emphasis added).[124] When deciding on the form of that "copy", controllers must therefore assess whether contextualising the personal data by providing exact copies or extracts from documents is necessary for data subjects to make sense of the information contained therein. If that is not the case, and provided that the provision of a "compilation" instead does not alter the substance and scope of the information, controllers can opt for that format.[125]

Modalities of the right of access–form of the answer

The modalities elicited in Article 12(1) GDPR equally apply to "any communication under Articles 15 to 22"; reference is therefore made, for that matter, to the above section on the form of the privacy/data policy. Since controllers are required to provide a copy of *all* the personal data processed, however, these standards might be more difficult to meet in case of large-scale or

all the more important since it was not included in Directive 95/46, the GDPR's predecessor, and therefore indicates a clear will from the legislator to add an extra dimension to the right of access.

[122] Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M, S* [2014] ECLI:EU:C:2014:2081, para 60.

[123] Case C-487/21 *FF v Österreichische Datenschutzbehörde* (n 25), paras 37, 38 and 41.

[124] ibid 45. It is also worth noting that, more recently, Advocate General Emilou referred to Case C-487/21 when answering, the third question in Case C-302/22 FT v DW (n 27) para 73, *i.e.*, "whether, in the context of a doctor-patient relationship, the phrase 'copy of the personal data undergoing processing' in the first sentence of Article 15(3) of the GDPR, should be interpreted as conferring on the data subject a general right to obtain a full copy of the documents included in his medical file".

[125] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 152. The wording used by the CJEU in Case C Case C-487/21 *FF v Österreichische Datenschutzbehörde* (n 25) para 45 ("that *right* entails" […], emphasis added) seems to suggests that, should data subjects request the provision of *exact copies of extracts from documents*, the onus is on the controller, according to the general principle of accountability, to demonstrate that such exact copies are not necessary to make sense of the data contained in the summary they provided instead, or that doing so would impede on the rights and freedoms of others as per Article 15(4) GDPR.

complex processing activities. The reference, in that provision, to the obligation to implement "appropriate" methods to provide that information, states the EDPB, therefore calls on controllers to "undertake great efforts" in such situations.[126] Read together with the accountability (Art.5(2)) and data protection by design (Art.25) narrative at the heart of the Regulation, controllers are now obliged to implement and – crucially – document the measures put in place to ensure effective compliance with data subject's rights.[127] If the satisfaction rate for the final answer substantially improved in 2022, going from 33% to 55% of participants being either "satisfied" or "very satisfied" (fig. 12), the most recurring issue they flagged was identical in both studies, namely that many OSPs provided raw, unintelligible data without any sort of additional information to decipher their meaning.

Just like the WP29 in its Guidelines on transparency, the EDPB advocates for a "layered" approach where the amount of personal data to be included in the "copy" potentially conflicts with the "intelligibility" and "conciseness" requirements.[128] Such an approach allows controllers to provide the information listed in Article 15(1) and (2) GDPR in different layers, the first one detailing what data subjects "would generally consider as most relevant", and each subsequent one adding more personal data, potentially in raw format.[129] It is also crucial that controllers share the necessary "keys" for data subjects to understand what each data entry corresponds to, especially if they use a proprietary encoding format, as well as the tools to render the datasets intelligible.[130] Using a "layered" approach, however, should be reserved to situations where data subjects would not be able to make sense of decontextualised data, and should not in any way limit the scope of the right of access nor create additional burden for individuals.[131] Which means, in turn, that data subjects are entitled to receive the additional layers containing the raw, more complex personal data should they so decide.

If, as outlined above, providing a "copy" is the main modality to fulfil their obligations under Article 15 GDPR, controllers are free to explore other options such as "oral information, inspection

[126] ibid 129, 140.
[127] See Articles 5(2), 24(1) and 25(1) GDPR. This is hinted at in ibid 126, 136.
[128] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 33) paras 35–38; European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) paras 141, and entire Section 5.2.4.
[129] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 145.
[130] ibid examples 27 and 28. See also, on that note, Ausloos, Mahieu and Veale (n 58) paras 28–38. The idea of making such tools available to the data subjects was also pitched in European Data Protection Board (n 14) para 149, noting that "[w]hen assessing if a format is a commonly used electronic format, the EDPB considers that it is of importance how easily the individual can access information provided in the current format". "In this regard", adds the Board, "it should be noted what information the controller has provided to the data subject about how to access a file which has been provided in a specific format, such as *what programs or software that could be used*, to make the format more accessible to the data subject" (emphasis added).
[131] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) paras 143, 147.

of files, [or] onsite or remote access without possibility to download".[132] The vast majority of controllers still preferred emails as the communication channel through which providing the said copy; 57% in 2020 and even raising to 78% two years later (fig. 19).[133] Self-service solutions in the form of direct consultation (11% in 2020 and 5% in 2022) and download tools (46% in 2020 and 38% in 2022) were also well represented. These are no silver bullet, though, as some of the elements listed in Article 15(1) and (2) GDPR might be missing.[134] Indeed, participants experienced difficulties when trying to complement the information made available on OSPs' platform or obtain clarifications on what was included in the downloaded file, as controllers would systematically answer these requests by referring to the said consultation and download tool. As noted by the EDPB, it is essential that these solutions are not used by controllers to "limit the scope of the personal data received".[135] In that sense, self-service tools, if used as the sole medium through which providing access, run the risk of having controllers unilaterally shape the contours of their obligations, and therefore altering data subjects' perception of what they are entitled to receive.

Finally, and as recalled by Article 15(3) GDPR, "where the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic form". What is considered a "commonly used electronic form", underlines the EDPB, "will vary over time" and should be based on "an objective assessment and not on what format the controller uses in its daily operations".[136] This will either be a format "generally used in the controller's area of operation", or, short of such an option, "an open format set in an international standard, such as ISO".[137] In any case, the chosen format should ensure that the information is presented to data subjects in an "intelligible" and "easily accessible" manner, as required by Article 12(1) GDPR. The "copy" should also "persist over time", which means that a written form is, in general, preferred over other formats, and that offering a mere consultation tool with no possibility to download the personal data displayed thereon is not sufficient.[138] In 2020, plain text was, by far, the most popular format used by controllers to provide access (54%), often in combination with .json (23%) and/or .pdf (20%) files (fig. 20).[139] This drastically changed two years later, as controllers

[132] ibid 133.
[133] Participants would select more than one option, which explains that the total adds up to more than 100%.
[134] See in this regard also: Jan Tolsdorf, Michael Fischer and Luigi Lo Iacono, 'A Case Study on the Implementation of the Right of Access in Privacy Dashboards' in Nils Gruschka and others (eds), *Privacy Technologies and Policy*, vol 12703 (Springer International Publishing 2021) <https://link.springer.com/10.1007/978-3-030-76663-4_2> accessed 24 November 2023.
[135] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) para 138.
[136] ibid 134, 148, 149.
[137] ibid 149.
[138] ibid 150, 151.
[139] As noted in Ausloos, Mahieu and Veale (n 41) para 23, controllers should not proactively convert data in machine-readable (*e.g.*, JSON, CSV) to an unstructured format such as PDF.

abandoned plain text in favour of structured, often machine-readable formats such as .xls(x) (40%), .pdf (26%), .csv (12%) or .json (10%), allowing the provision of more granular information – if sometimes, as noted above, at the cost of intelligibility.

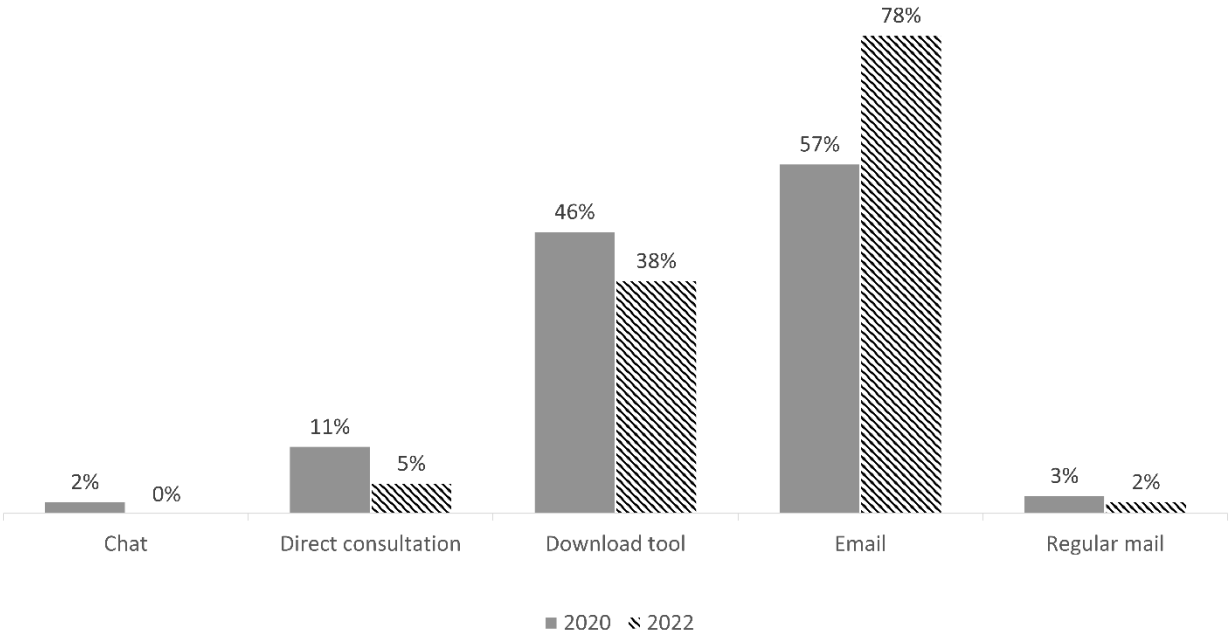

Figure 19 - Medium through which OSPs provided access

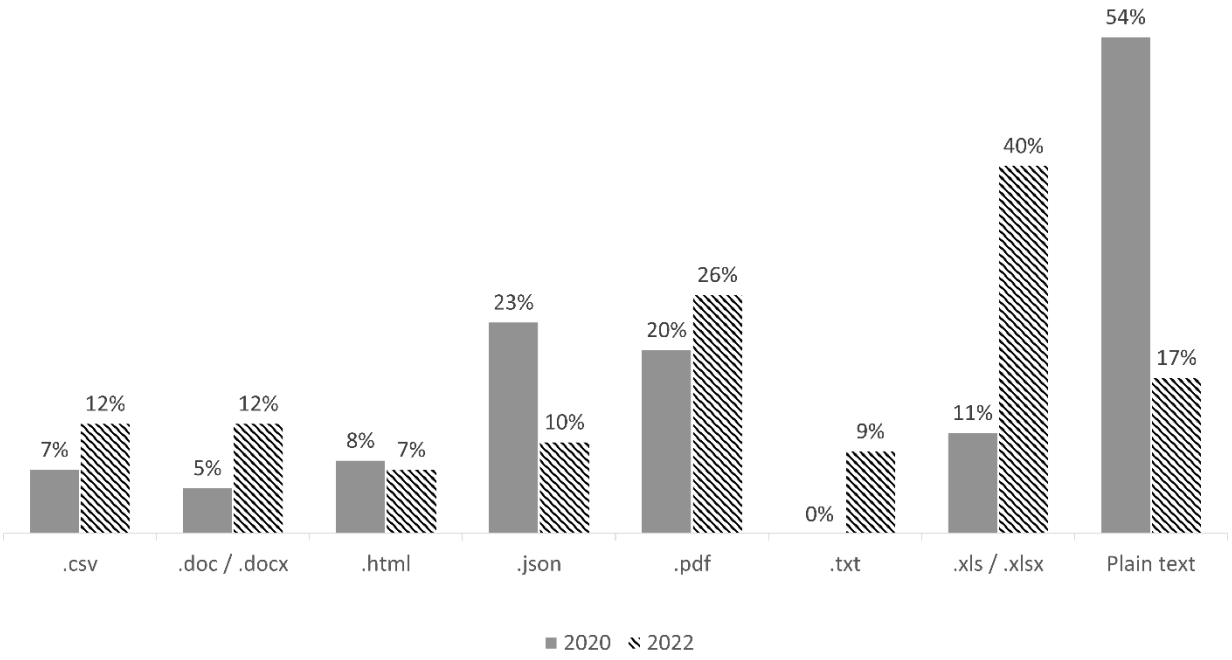

Figure 20 - Format used by OSPs to provide access

V. CONCLUSION: THE CURRENT STATE OF ACCESS

The Good. Looking at the evolution of controllers' compliance with the right of access in general, there seems to be progress across the board, and the situation has come a long way since the entry into force of the GDPR. When compared to the results outlined in older empirical studies, including the one we conducted back in 2017, it appears that OSPs have improved on many points. Whereas before 2018, many controllers were not even aware of the right of access, let alone its scope and meaning, all controllers are now up to speed with the basics of Article 15 GDPR. This is undoubtedly the result of the media attention the GDPR received right after it became applicable, the emergence of similar rights across the world,[140] including in California,[141] and the growing amount of people and organisations (collectively) exercising the right of access. As a result, we also observe a certain degree of professionalisation of the right of access over time, with especially large OSPs developing internal procedures (*e.g.*, dedicated response teams) and technical tools (*e.g.*, data download functions) to accommodate data subjects' prerogatives. While this has improved compliance, these efforts also demonstrate the intense regulatory entrepreneurship OSPs are undertaking to try and shape the scope of the right of access.

The Bad. Our empirical findings reveal that many OSPs tend to provide, at least at first instance, boilerplate answers when confronted to access requests formulated according to Article 15 GDPR. Arguably in an attempt to somewhat automate compliance with their duties under the GDPR. These often consists of copy-pasted text extracted straight from their privacy/data policy or refer to data download functionalities where available. We also noted that these self-service tools generally provide lacunary information and can only be accessed by registered users. Arguing against these practices proved particularly cumbersome, time-consuming, and sometimes counterproductive. We therefore welcome the clarification of the EDPB that the information given under Article 15 must be tailored to the individual case of the data subject and relate to the specific processing operations involved. This is precisely the added-value of Article 15 when compared to Articles 13 and 14 GDPR.[142] The CJEU recently hammered on that point when ruling that "the information provided to the data subject pursuant to the right of access provided for in Article 15(1)(c) of the GDPR must be as *precise* as possible", and that the "right of access entails

[140] Graham Greenleaf, 'Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021)' (2021) 169 Privacy Laws & Business International Report 6 <https://papers.ssrn.com/abstract=3836261> accessed 10 November 2021.
[141] California Consumer Privacy Act of 2018 (CCPA) (28 June 2018) <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5> accessed 30 June 2023.
[142] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 19) paras 37–41.

the ability of the data subject to obtain from the controller information about the *specific* recipients to whom the data have been or will be disclosed" (emphasis added).[143]

Summing up, OSPs have clearly invested in GDPR compliance processes – which has benefitted data subjects to some extent. We noticed an overall increase in satisfactory answers. If these are not merely "symbolic structures" as some have claimed,[144] there is certainly still a lot of room for improvement. Notably, we were baffled by the fact that, in 2022, a fifth of OSPs still did not provide any relevant privacy- or data protection-related information during the registration process. In the same vein, more than a quarter of OSPs failed to offer non-registered data subjects the possibility to request access to their personal data through a publicly accessible contact forms, or a dedicated data download functionality. As pointed out in earlier, we also observed an increase in the time OSPs took to respond to access requests, with 36% (in 2020) to 50% (in 2022) taking more than a week to provide a first substantive answer. Not just that, 51% (in 2020) to 77% (in 2022) failed to respect the one-month time limit of Article 12(3) GDPR, while 10% (in 2020) to 15% (in 2022) of OSPs did not even bother to respond at all, despite multiple reminders. This, we believe, is symptomatic of a broader lack of consideration for the modalities of access in general.

The Challenges Ahead. Taking a step back, we believe that one of the points that deserve the most attention from regulators and judicial authorities is controllers' deliberate attempts at curtailing the scope and meaning of access rights.[145] Indeed, and while we noticed considerable improvements throughout both our studies, we also noted a certain rigidity settling in, with OSPs only routinely accommodating *parts* of our access requests, providing boilerplate responses, exceeding legal delays and complicating non-automatable requests (*e.g.*, by non-registered data subjects). Unless we want to see the right of access being gradually watered down, active pushback is necessary. The recent EDPB guidance is helpful – confirming a wider interpretation than how OSPs often operationalise access rights compliance in practice – but insufficient. Continued use of access rights and strategic challenges to narrow interpretations are vital. Moreover, we hope that data protection authorities will become more proactive in enforcing access rights rules.[146] Adequate compliance with access rights will have a trickle-down effect,

---

[143] Case C-154/21 *RW v Österreichische Post AG* (n 26) para 43.

[144] Ari Ezra Waldman, *Industry Unbound: The inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021) 131–132.

[145] An approach that same have coined "regulatory entrepreneurship". See, on that notion: Elizabeth Pollman and Jordan Barry, 'Regulatory Entrepreneurship' [2017] Southern California Law Review <https://scholarship.law.upenn.edu/faculty_scholarship/2556>.

[146] Recently the French Commission Nationale de l'Informatique et des Libertés (CNIL) issues a €40 million fine against AdTech company Criteo, *inter alia* for failing to properly accommodate the right of access. Importantly though, this case is the result of sustained efforts by civil society that have pressured the DPA for five years until a decision was issued. See: Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO [2013] <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047707063> accessed 30 June 2023.

enabling the safeguarding of other data protection rights, as well as a broader range of rights, freedoms, and interests.[147] Litigation will play a crucial role in that regard. In that sense, it is good to see the European Commission taking active steps to harmonise the procedural rules for the enforcement of cross border cases, [148] and commit to monitoring the progress of large-scale enforcement actions.[149]

[147] Laurens Naudts, Pierre Dewitte and Jef Ausloos, 'Meaningful Transparency through Data Rights: A Multidimensional Analysis' [2022] Research Handbook on EU Data Protection Law 530; René Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020) <https://policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487> accessed 7 July 2020; René Mahieu, 'The Right of Access to Personal Data in the EU' (n 11).

[148] See European Commission, 'Proposal for a Regulation of the European Parliament and of The Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 (n 13).

[149] See the Comments of the European Commission on a follow up from the European Ombudsman on how it responded to concerns that it collects insufficient information about Ireland's implementation of the EU's General Data Protection Regulation (GDPR) <https://www.ombudsman.europa.eu/en/doc/correspondence/en/165453> accessed 30 June 2023. That commitment follows the decision from the European Ombudsman in case 97/2022/PB initiated by the Irish Council for Civil Liberties (ICCL). For more information, see: How the European Commission responded to concerns that it collects insufficient information about Ireland's implementation of the EU's General Data Protection Regulation (GDPR) <https://www.ombudsman.europa.eu/en/case/en/60860> accessed 30 June 2023.