Centre for Information Policy Leadership
HUNTON

A Single Standard for Anonymisation

Article 6(11)DMA, the GDPR, and Expectations of Europeans

July 2026

EXECUTIVE SUMMARY

Article 6(11) of the Digital Markets Act (DMA) requires providers of designated gatekeeper search services to make ranking, query, click and view data available to third-party online search engine providers on fair, reasonable and non-discriminatory (FRAND) terms. Any data constituting personal data is to be anonymised prior to sharing. The objective, contestability in the search market, is important and legitimate, and CIPL[1] supports both the objective and the data sharing the provision mandates. This paper does not address *whether* search data should be shared in the context of Article 6(11) DMA, but what the standard of anonymisation should be, going forward.

That same question is currently being considered in real time across three workstreams that are not always in step. In specification proceedings (DMA.100209), the Commission adopted preliminary findings on 16 April 2026, giving the undefined anonymisation requirement in Article 6(11) concrete meaning for the first time, in a competition-enforcement setting, with a binding decision due by 27 July 2026. In parallel, the GDPR benchmark itself is in motion: since the Court of Justice's 2025 judgment in *Single Resolution Board v EDPS* adopted a relative, recipient-focused approach to identifiability, the European Data Protection Board has just published draft guidance revising the anonymisation framework and now open for consultation[2], and the Digital Omnibus proposes legislative amendments bearing directly on how anonymisation and pseudonymisation are defined. Absent genuine coordination, "anonymised" risks being settled differently in the DMA-enforcement context, under the GDPR, and potentially under the DSA and the Data Act as well.

Instead, Article 6(11) should be implemented on a single, GDPR-consistent standard of anonymisation. The DMA is based solely on Article 114 TFEU and is not *lex specialis* to the GDPR; the two instruments apply without prejudice to each other and must be applied compatibly. Implementation of a market-regulation instrument must not diverge from the level of protection afforded by a fundamental rights instrument anchored in the EU Charter. A bespoke, DMA-specific meaning of 'anonymised' would create two standards for a single concept — one calibrated to the internal market and one to fundamental rights — generating legal uncertainty and running contrary to the wider goal of simplification across the EU digital acquis.

The paper is also informed by a six-market consumer survey CIPL conducted in partnership with the European Public Policy Partnership (EPPP), completed in May 2026, gathering the views of over 3,000 respondents in Slovakia, Germany, France, Ireland, Estonia and Spain. The findings underscore both why the standard matters and where user expectations sit in this context.

---

[1] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] The European Data Protection Board, Guidelines 02/2026 on Anonymisation, available at https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf.

Unlike data portability under the GDPR or Article 6(9) DMA, the sharing in the context of Article 6(11) DMA is neither initiated nor approved by the user. And the data shared is generated by an activity that almost everyone engages in almost every day. A consumer perspective can therefore provide valuable insights when assessing how to balance DMA and GDPR.

Key findings of the CIPL–EPPP consumer survey (n=3,045; six EU markets, May 2026)

Search is near-universal: 90% of respondents use a search engine at least once a day (82% in Germany to 95% in Spain). AI chatbots complement rather than displace search: for quick answers, 60% rely mostly on traditional search engines, 12% turn to chatbots.

Sensitive queries in search: 44% searched for health and medical information in the past month, 27% for financial information, 26% for personal life and 12% for sensitive personal beliefs; 59% use search for sensitive or intimate topics often, 37% make use of chatbots.

A strong expectation of confidentiality: 66% expect their search history to remain confidential between themselves and the provider (51%–76% across markets).

Low awareness of sharing obligation: 71% were unaware that EU legislation such as the DMA may require certain search engines to share search data with competing providers.

Scepticism about anonymisation: Acceptability of sharing anonymised data is split almost evenly (35% acceptable, 36% unacceptable). But 50% consider it likely that anonymised search data could be re-identified and linked back to them; only 16% consider this unlikely.

Users look for agency: If given a choice, 51 % of users would want to be able to opt out, 41% to actively consent; 31% look for more information.

Against this background, the paper makes five recommendations:

1. **Implement Article 6(11) on a single, GDPR-consistent standard of anonymisation that applies consistently across the digital acquis.**

The term "anonymised" in Article 6(11) DMA should carry the meaning it has in the GDPR context: whether identification of a natural person is reasonably possible, taking into account all the means reasonably likely to be used (Recital 26 GDPR), as confirmed by the Court of Justice in *SRB* and continues to be developed in the EDPB's guidance (and ultimately as part of the Digital Omnibus). A bespoke, DMA-specific application, whether more permissive or more restrictive than the GDPR's, would create two standards for a single concept, one calibrated to the internal market and one to fundamental rights, generating legal uncertainty and running contrary to the simplification objectives across the digital acquis. The standard settled in the Article 6(11) context should be applicable consistently across the GDPR and the digital acquis.

2. **Apply a relative, risk-based assessment.**

Consistency with the GDPR does not mean importing a zero-risk standard. Following *SRB*, identifiability is assessed by reference to the means reasonably likely to be used by the actual recipient, its capabilities, auxiliary data and context, not by hypothetical, unlimited adversaries. Re-identification should be made unlikely, not impossible in the abstract.

3. **Anchor anonymisation in robust technical measures, with contractual and organisational safeguards reinforcing them.**

There is a difference in kind between measures that change what the data is and measures that govern what a recipient may do with it. Technical de-identification, including privacy-enhancing technologies such as differential privacy, synthetic data generation and generalisation, should carry the decisive work of reducing identifiability. Contractual and organisational safeguards — prohibitions on re-identification and linkage, purpose limitation, retention limits, onward-sharing restrictions and independent audit — are valuable accountability instruments that CIPL has long supported, and they properly reinforce a technically sound outcome and guard against downstream misuse. Whether proposed measures strike the right balance towards an acceptable standard should be determined by the Commission and data protection authorities together, with the involvement of technical experts; and the balance accepted there should then hold reciprocally in the GDPR context.

4. **Coordinate the three workstreams shaping "anonymised" to avoid fragmentation.**

The meaning of anonymisation is currently being determined administratively (DMA.100209), interpreted judicially and in draft EDPB guidance, and reshaped legislatively through the Digital Omnibus — in parallel and not always in step. Regulatory cooperation between the Commission, the EDPB and national DPAs should ensure that DPA expertise is reflected in binding specification measures. If coordination between the institutions cannot deliver a single standard, resolving the question may ultimately fall to the legislator — through the Digital Omnibus or an implementing act — to prevent divergent understanding and standards from consolidating. Regardless, meaningful outcomes will require strong stakeholder involvement on both the sharing and the receiving side of Article 6(11).

5. **Consider the end user in the implementation of Article 6(11), and bring users on the journey.**

The individuals whose data is shared are not a party to the regulatory dialogue, and the sharing in the context of Article 6(11) is neither initiated nor approved by the user. The CIPL–EPPP six-market survey shows a discrepancy: 66% of Europeans expect their search history to remain confidential, 71% are unaware of the DMA sharing obligation, half believe anonymised data could be re-identified and look for agency. Within the structure of Article 6(11) as it stands, transparency is the most tangible means of closing that trust gap. As Article 6(11) is implemented, consideration should be given to measures by stakeholders that promote greater clarity around how users' search interactions relate to the data-sharing regime, including accessible information about third parties that may be granted access.

TABLE OF CONTENTS

I. INTRODUCTION

The Digital Markets Act (DMA) entered into force in November 2022 and became fully applicable to designated gatekeepers in 2024.[3] The Centre for Information Policy Leadership (CIPL) has engaged extensively in interpreting certain DMA provisions, in particular regarding their interplay with the GDPR.[4]

Some of the more complex questions on the interplay of the DMA and GDPR have emerged in the context of the DMA's data portability obligations.[5] Among those is Article 6(11), which compels the providers of designated search engines that fall into the gatekeeper definition of the DMA[6] to make their search data[7] available to third parties on fair, reasonable and non-discriminatory terms (FRAND). The objective of Article 6(11) is contestability in the search market: addressing the barriers to entry prospective search engines may face.[8]

As the European Data Protection Supervisor pointed out in its DMA Opinion,[9] such data sharing may inevitably also include personal data provided by the end user, for instance, in search queries when the individual enters personal data as part of a search, or data that the end user generated through the use of the gatekeeper's respective core platform service.

On 16 April 2026, two years into the DMA's full applicability, the European Commission adopted preliminary findings in specification proceedings, setting out the measures it considers necessary for compliance with Article 6(11) in practice.[10] Those measures were subject to public consultation, with

[3] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L 265, 12.10.2022.

[4] For CIPL's body of work on the Digital Markets Act, see the Centre for Information Policy Leadership, https://www.informationpolicycentre.com/project/digital-markets-act/.

[5] See in particular CIPL's work on Article 6(9) DMA, which sets out proposals for proceeding with data-access obligations while protecting the fundamental rights of individuals: CIPL, *Data Sharing Obligations Under the DMA: Challenges and Opportunities* (May 2024), available at https://www.informationpolicycentre.com/resources/data-sharing-obligations-under-the-dma-challenges-and-opportunities/.

[6] Under Article 3 DMA, an undertaking is designated a gatekeeper where it (i) has a significant impact on the internal market, (ii) provides a core platform service that is an important gateway for business users to reach end users, and (iii) enjoys an entrenched and durable position (or is foreseeably about to acquire one). Article 3(2) DMA sets rebuttable quantitative presumptions for each limb, including annual EEA turnover of at least EUR 7.5 billion in each of the last three financial years (or an average market capitalisation of at least EUR 75 billion), together with a core platform service having at least 45 million monthly active end users in the EU and at least 10,000 yearly active business users. To date, Alphabet is the only undertaking designated as a gatekeeper for an online search engine within the meaning of the DMA, and therefore the only entity to which Article 6(11) currently applies (Commission Decision of 5 September 2023 designating Alphabet Inc. as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925, Case DMA.100013).

[7] The DMA does not define "search data" as a standalone term, but Article 6(11) DMA specifies that "ranking, query, click and view data in relation to free and paid search generated by end users on [the gatekeeper's] online search engines," to which third-party online search engine providers must be granted access on fair, reasonable and non-discriminatory terms, with any data constituting personal data anonymised.

[8] DMA Recital 61 frames the Article 6(11) obligation as addressing the structural advantage that incumbent search engines derive from accumulated query data, with the aim of enabling third-party online search engines to improve their services.

[9] EDPS Opinion on the European Commission's proposal for a Digital Markets Act, available at https://www.edps.europa.eu/data-protection/our-work/publications/opinions/digital-markets-act_en.

[10] European Commission, *DMA.100209 – Consultation on the proposed measures for Google Search data sharing (Article 6(11) of the DMA)*, 16 April 2026, https://digital-markets-act.ec.europa.eu/dma100209-consultation-

a binding decision to be issued by 27 July 2026. This paper takes that debate and the ongoing proceedings as its backdrop rather than its subject.

To date, public and regulatory debate around Article 6(11) DMA has been centred on contestability. This paper is instead focused on a question at the interplay between the DMA, the GDPR and the wider EU digital acquis: Article 6(11) requires that search data which constitutes personal data within the scope of the GDPR be anonymised before it is shared. Recital 61 DMA reinforces this, requiring gatekeepers to guard against re-identification by *appropriate means*, while making equally clear that those measures should *not substantially degrade the usability* of the data made available to third parties. This raises two questions: first, whether the standard of anonymisation under Article 6(11) DMA should be the same as understood in the context of the GDPR. Second, where the minimum threshold of data utility lies, i.e. how far the identifiability can be reduced before the data cease to be valuable for the contestability purposes the DMA pursues.[11]

The contestability objective of the DMA is important and legitimate.[12] At the same time, the manner in which the obligation is implemented should ensure that it does not establish a bespoke, DMA-specific approach for the notion of "anonymised" that diverges from, or may sit below, the meaning given to the same term in the GDPR context. This would risk creating two standards for a single concept: one calibrated to the functioning of the internal market and one to the protection of fundamental rights, ultimately leading to legal uncertainty, and contrary to the wider goal of simplification across the EU's digital acquis. The argument developed throughout this paper is that Article 6(11) should be implemented on a single, GDPR-consistent standard of anonymisation in coordination with all relevant stakeholders. This is not to suggest that the current anonymisation standard under the GDPR is or should be immutable,[13] but anonymisation should be understood and applied consistently under the various instruments.

The paper is structured as follows. Section II sets out CIPL's consideration around Article 6(11), and why this provision is a distinctive case within CIPL's broader call for consistency across the EU digital acquis. Section III sets out why the question matters in practice, drawing on consumer responses from our study. Section IV turns to the data protection dimension and the central role of the anonymisation standard. Section V considers what a single, GDPR-consistent standard would require, and the part that technology, recipient governance and transparency play in delivering it. Sections VI sets out CIPL's recommendations, and the Annex provides the more detailed survey results.

---

proposed-measures-google-search-data-sharing_en. The Commission is required to adopt a binding decision by 27 July 2026.

[11] See CIPL "When the dust settles: Remaining Questions of Privacy vs Utility under the DMA", available at https://www.euractiv.com/opinion/when-the-dust-settles-remaining-questions-of-privacy-vs-utility-under-the-dma/.

[12] See CIPL, *Data Sharing Obligations Under the DMA: Challenges and Opportunities* (May 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_sharing_obligations_under_the_dma_-_challenges_and_opportunities_-_may24.pdf, CIPL recognises the legitimacy of the DMA's contestability objective but stresses that its implementation must protect individuals and preserve trust in the digital ecosystem.

[13] For example, please see CIPL Response to the European Data Protection Board's Public Consultation on Draft Guidelines 01/2025 on Pseudonymisation, available at https://www.informationpolicycentre.com/resources/cipl-response-to-the-european-data-protection-boards-public-consultation-on-draft-guidelines-01-2025-on-pseudonymisation/.

II. THE NEED FOR CONSISTENCY ACROSS THE DIGITAL ACQUIS WITH ARTICLE 6(11) AS THE TEST CASE

A recurring tenet in CIPL's work on the DMA has been that DMA obligations cannot be read in isolation, or only from the gatekeeper's perspective, but that they must be implemented compatibly with the GDPR and the wider body of EU digital law.[14]

This is not specific to any one provision. It reflects a broader position CIPL has consistently taken – the EU's digital instruments (the GDPR, the Digital Markets Act, the Digital Services Act, the Data Act, the AI Act, NIS2, DORA, and now the Digital Omnibus amendments) should be applied as a coherent whole rather than as a set of regimes that pull in different directions.[15] Where the same concept appears in more than one instrument, it should, so far as the law allows, carry the same meaning. Fragmentation of core concepts across instruments produces legal uncertainty, raises compliance complexity, and erodes the predictability on which both regulated entities and individuals depend.

Article 6(11) DMA as the test ground

Article 6(11) DMA is a particular example of the need for consistency across the EU Digital Acquis. The GDPR itself does not offer a definition for anonymisation. Instead, the interpretation provided by data protection authorities (DPAs) has been setting a high bar for anonymisation, including making the deletion of the original dataset a condition for rendering the dataset irreversibly anonymous,[16] which is obviously not an option in the context of data sharing under Article 6(11) DMA.

In a more recent publication, the Spanish AEPD and the EDPS issued a joint paper to clarify the DPAs' understanding of properly anonymised data further. The paper emphasises that, from a data protection point of view: "*100% anonymisation in a strict sense is the aim*," but it concedes that this may not always be possible.[17] The conclusion reached by the AEPD and the EDPS for such cases is that controllers have to "choose between processing personal data (and use, e.g., pseudonymisation) and apply the GDPR, or not to process the data at all." In the context of the DMA, this is also not an option.

The Commission, in its proposed measures in relation to Art. 6(11) DMA suggests a two-tier threshold: technical measures (suppression of direct identifiers, precise timestamps and generalisation of metadata such as location and device, etc.) are designed to reduce the likelihood of re-identification of end users to a "residual level;" contractual and organisational measures — a prohibition on re-identification and on linking the dataset with auxiliary data, purpose limitation to search-engine

[14] CIPL has consistently emphasised that DMA obligations involving personal data must be interpreted and applied compatibly with the GDPR, and that the EU's digital-market and data-protection rules should be read together as part of a coherent acquis rather than in isolation.

[15] A concrete example of this alignment is already taking shape in the single-entry point for incident reporting proposed under the Digital Omnibus, which would let an organisation report an incident once and have it routed to the competent authorities under the GDPR, NIS2, DORA and related instruments — building efficiencies for organisations while giving individuals a clearer and more consistent account of how incidents affecting them are handled

[16] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[17] AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation, available at https://www.edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en

optimisation, infrastructure separation from advertising and analytics data, retention limits, no onward sharing and independent assurance/audit — are designed to reduce that residual likelihood further to an "insignificant level."[18] In the Commission's formulation, however, it would appear that the decisive step from "residual" to "insignificant" is currently carried not by technical anonymisation levels, but by the contractual and organisational layer governing the recipient.[19] While every anonymisation process will involve some reliance on governance to manage residual risk, the question to arbitrate is the appropriate balance between both. Such an approach should then also be applicable in the context of the GDPR.

Additional uncertainty comes from the fact that the meaning of "anonymised" is being considered at present, in real time: under the DMA specification proceedings, but also across two other workstreams that are proceeding in parallel and not always in step with one another:

- **The DMA specification process.** In DMA.100209, the Commission is, for the first time, giving the undefined anonymisation requirement in Article 6(11) concrete meaning through proposed binding measures.[20] The substance of what "anonymised" requires is, in practice, being determined, in a competition-enforcement setting, with a particular focus on technical and contractual measures.
- **The evolving GDPR standard.** The benchmark against which any anonymisation measure must be judged is itself in motion. The Court of Justice's 2025 judgment in *Single Resolution Board v EDPS* adopted a relative approach to identifiability, assessing whether data is personal by reference to the means reasonably likely to be used by the actor in question[21], and the European Data Protection Board has just issued draft guidance revising the existing anonymisation framework in light of that judgment and a decade of technical change.[22]
- **The legislative layer.** The Digital Omnibus process proposes amendments to several EU digital instruments, including the GDPR, that bear directly on how anonymisation (and pseudonymisation) are defined.[23] The concept is therefore being shaped legislatively at the same time as it is being applied administratively and interpreted judicially.

---

[18] European Commission, Consultation on the proposed measures for Google Search data sharing (Article 6(11) of the DMA), available at https://digital-markets-act.ec.europa.eu/dma100209-consultation-proposed-measures-google-search-data-sharing_en.

[19] European Commission, *Preliminary Measures*, Case DMA.100209 – Alphabet – Article 6(11) – Google Search Data Sharing, para. 19, distinguishing "technical measures" that "mitigate the risk of re-identification of end users to a residual level" from "contractual measures [that] complement the technical measures and further mitigate the residual risks of re-identification of end users to an insignificant level." See also European Commission, *Case Summary*, Case DMA.100209, section on Anonymisation.

[20] European Commission, *DMA.100209 – SP – Alphabet – Article 6(11) Google Search Data Sharing: Case Summary*, 16 April 2026. The Commission opened specification proceedings under Article 8(2) DMA on 27 January 2026 and adopted its preliminary findings on 16 April 2026.

[21] Judgment of 4 September 2025, *European Data Protection Supervisor v Single Resolution Board*, C-413/23 P, on the relative concept of personal data and the assessment of identifiability from the perspective of the recipient, building on *Breyer* (C-582/14).

[22] The European Data Protection Board, Guidelines 02/2026 on Anonymisation, available at https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf.

[23] European Commission, *Proposal for a Regulation amending the GDPR and other EU digital rules* ("Digital Omnibus"), pending. The proposal bears on the anonymisation question through, among other things, the treatment of pseudonymised data and a task for the Commission to specify, by implementing act, the means

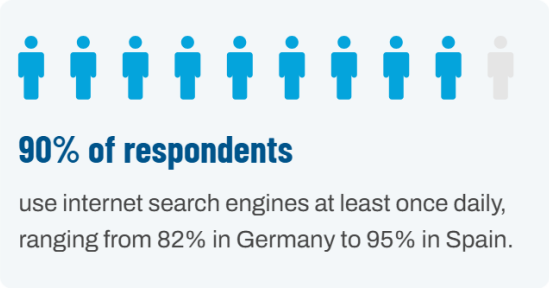
The Commission, the EDPB and the Court of Justice, together with the co-legislators, each hold a piece of the same concept in parallel. That fragmentation complicates any approach to Article 6(11) DMA: it leaves open both the question of what counts as sufficiently anonymous and the question of who should ultimately arbitrate the trade-off between privacy and utility. Absent genuine coordination, "anonymised" risks being settled differently in the DMA-enforcement context than it does under the GDPR, and potentially under the DSA and the Data Act as well, with the consequences outlined above. This may ultimately be a matter for the legislator to ensure a unified approach.

III. WHY IT MATTERS: SEARCH REMAINS WIDELY USED

Given changing consumer habits, for the purpose of this paper, CIPL wanted to understand what role search continues to play in consumers' everyday use of applications, in particular, given the increasing popularity of generative AI applications.[24] Our study outcome suggests that search engines continue to be the primary channel through which individuals seek information. While AI chatbots have emerged as an additional means of accessing information, the evidence indicates that they have largely complemented, rather than displaced, traditional search.

1. Search is a daily, near-universal activity

Internet search is part of the daily routine of almost every respondent. Across the six markets surveyed, 90% of respondents reported using a search engine at least once a day, ranging from 82% in Germany to 95% in Spain, with a large majority using search engines several times a day.[25] While the digital economy, including search, has been going through numerous changes, the search box remains one of its most heavily used entry points.



and criteria for determining whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.

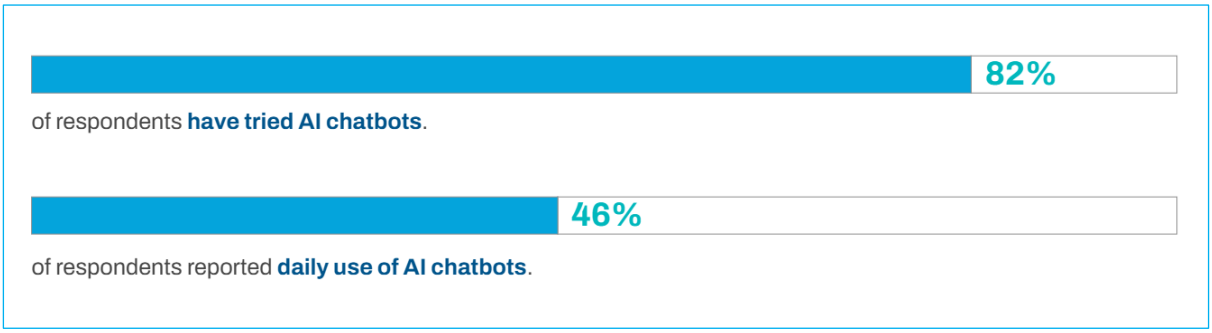
[24] According to Eurostat, in 2025 some 32.7% of individuals aged 16–74 in the EU had used generative AI tools in the previous three months, mostly for personal purposes (25.1%), with adoption highest among 16–24 year-olds (around 64%). Use varied considerably across Member States, from 48.4% in Denmark to 17.8% in Romania. See Eurostat, *Use of artificial intelligence by individuals*, Statistics Explained (2025), available at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_by_individuals.

[25] EPPP DMA Awareness Survey, *Q2: How often do you typically use internet search engines? An internet search engine is an online service (e.g. Google, Bing, etc.) where you can enter keywords or questions to find information on the internet. As a result, it shows you a list of relevant links.T2B = Multiple times a day + Once a day* (n=3,045). Daily use of internet search engines (top-two-box: multiple times a day plus once a day) totalled 90%, ranging from 82% in Germany to 95% in Spain; full country details in the Annex.

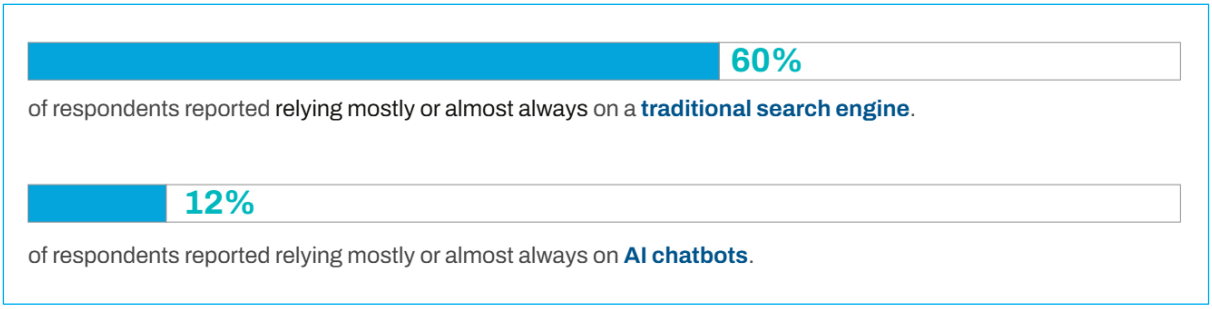
The data ultimately subject to Article 6(11) is therefore generated by an activity that almost everyone engages in, almost every day.

2. AI chatbots are growing in relevance, but at this stage have not displaced search engines

AI chatbots are clearly a fast-growing market segment.[26]



Especially when asked about their preference for quick search, 60% of respondents said they still rely mostly on a traditional search engine, compared with 12% who said the same for AI chatbots; roughly a quarter use both about equally.[27] This may change in the future: as search engines increasingly surface generative-AI summaries and AI applications draw on live search indices, the distinction may become less clean.



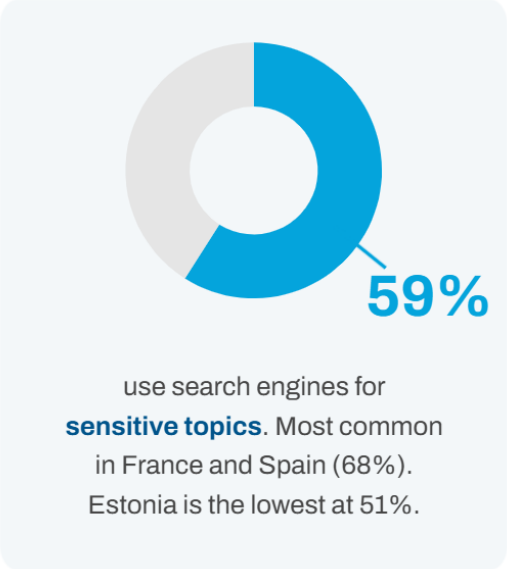
For sensitive or intimate topics (health, finances, personal life, personal beliefs), 59% of respondents said they often or almost always turn to a search engine (rising to 68% in France and Spain), compared with 37% for AI chatbots.[28]

---

[26]EPPP DMA Awareness Survey, Q3 (n=3,045) and Q4 (n=2,493). 82% of respondents reported having used AI chatbots; among users, 46% reported daily use. *Q3. Have you ever used generative artificial intelligence tools - AI chatbots? An AI chatbot is a conversational service (e.g. Gemini, ChatGPT, etc.) that can answer your questions, write texts, summarise documents, or create new content. You communicate with it similarly to how you would with a person via chat; Q4. How often do you typically use generative artificial intelligence tools - AI chatbots (e.g. ChatGPT, Gemini, etc.)? T2B = Multiple times a day + Once a day.*

[27]EPPP DMA Awareness Survey, Q5b (n=3,045). For quick answers, 60% reported relying mostly or almost always on traditional search engines, against 12% for AI chatbots; roughly a quarter reported using both about equally. *Q5b. Would you say that when searching for information, or getting quick answers to questions, you more often use traditional internet search engines (e.g. Google, Bing, etc.), or AI chatbots (e.g. Gemini, ChatGPT, etc.)?*

[28]EPPP DMA Awareness Survey, Q6_1 and Q6_2 (n=3,045). 59% reported using search engines often or almost always for sensitive or intimate topics (rising to 68% in France and Spain), against 37% for AI chatbots. *Q6_1. To what extent do you use internet search engines or AI chatbots to ask questions about sensitive or intimate topics*



3. What Europeans search for

CIPL was also interested in understanding what respondents search for. Asked which topics they had searched in the past month, respondents picked everyday information (62%), shopping (52%) and hobbies and interests (49%) most often, but a large share also chose more sensitive and intimate categories of data: 44% picked health and medical information, 27% picked financial information, 26% personal life, and 12% sensitive personal beliefs.[29] Health information thus features in the recent search history of nearly half of all respondents.[30]

Search queries are not all the same. A small set of high-frequency or 'fat-head' queries accounts for much of the total volume, while the 'long tail' of rarer and unique queries is where most of the competitive value of search data sits. At the same time, this is also where the privacy exposure may be greatest. Long-tail queries are more likely to be distinctive enough to single out an individual, and they may concern sensitive matters such as health, finances, sexuality or religion. The categories of data that make the long tail valuable for contestability are therefore the very categories that make robust anonymisation both important and a challenge, where the aim is to maintain the balance between anonymisation and data utility. Additionally, queries inevitably also contain personal data within the query text itself, which will frequently relate not only to the user, i.e. the person searching, but to identifiable third parties named in the query.[31]

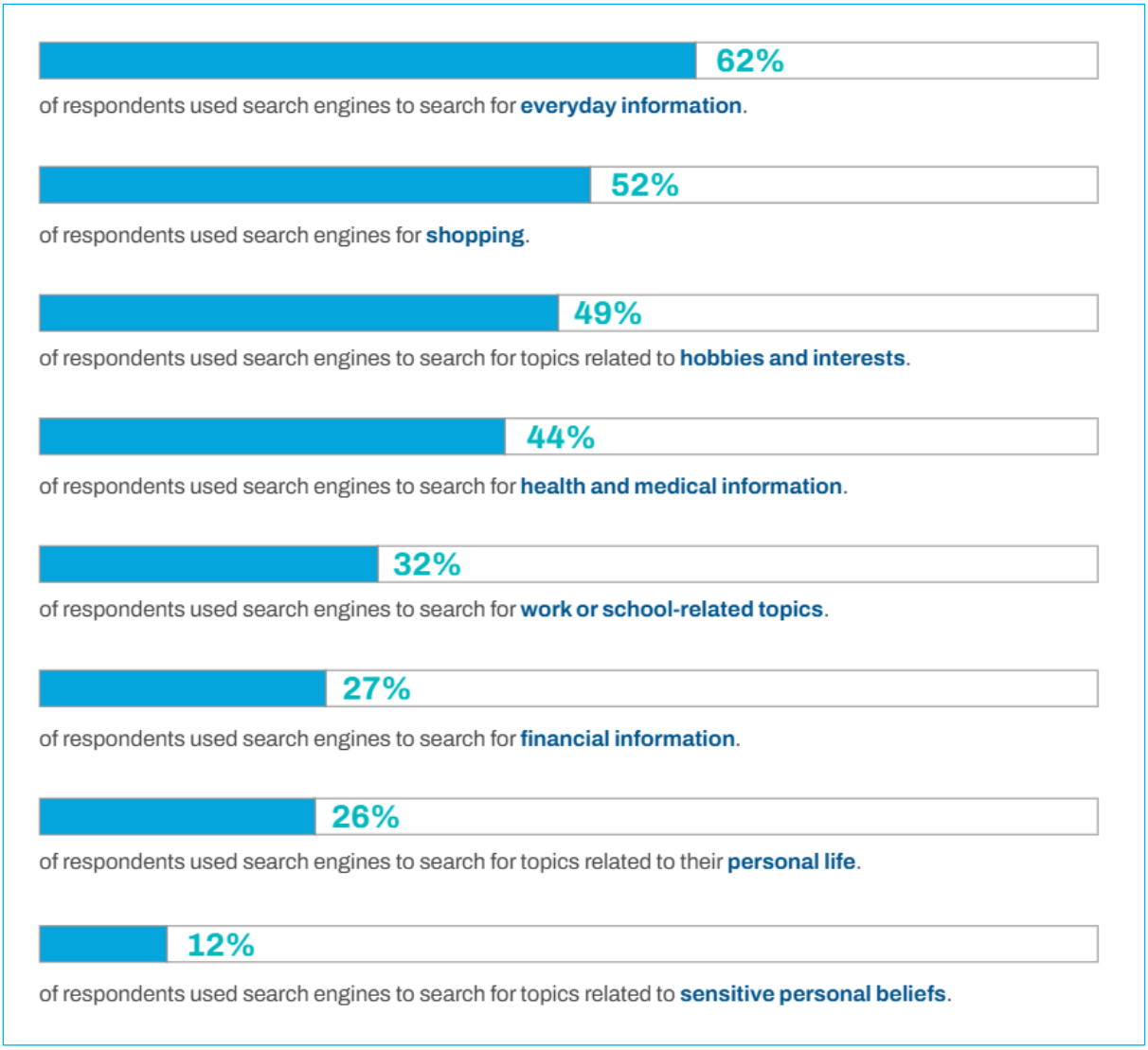
---

for you (such as health, finances, personal life, or your personal beliefs)? T2B = Almost always + Often, B2B = Rarely + Not at all; Q6_2. To what extent do you use internet search engines or AI chatbots to ask questions about sensitive or intimate topics for you (such as health, finances, personal life, or your personal beliefs)? T2B = Almost always + Often, B2B = Rarely + Not at all.

[29] EPPP DMA Awareness Survey, Q7 (n=2,493; respondents who searched in the past month). Topics searched in the past month: everyday information 62%, shopping 52%, hobbies and interests 49%, health and medical information 44%, work or school topics 32%, financial information 27%, personal life 26%, sensitive personal beliefs 12%. Ireland reported the highest shares for personal life (31%) and sensitive personal beliefs (18%).

[30] For a further breakdown by market, please refer to the Annex.

[31] Centre for Information Policy Leadership, *Data Sharing Obligations Under the DMA: Challenges and Opportunities*, CIPL Discussion Paper, May 2024, p. 6.



4. Europeans expect their searches to remain confidential

CIPL wanted to understand the sentiments of respondents regarding the treatment of their search data. The survey showed that users have strong expectations regarding this. Across the surveyed markets, 66% of respondents indicated that they expect their search history to remain confidential between themselves and the provider of the search service.[32] That expectation was consistently observed across all markets, ranging from 51% to 76%.[33]

[32] EPPP DMA Awareness Survey, Q7a (n=3,045). 66% expect their search history to remain confidential between themselves and the service provider (highest in Spain at 76%, lowest in Estonia at 51%); *Q7a. When you use an internet search engine or an AI chatbot, to what extent do you expect your individual search history to remain confidential between you and the providers of the service? T2B = Completely expect + Mostly expect, B2B = Completely do not expect + Mostly do not expect.*

[33] The corresponding figure for AI chatbots was 60%; see the Annex for more detailed information.

In a follow-up question, the survey tried to gauge whether respondents were aware that their search data might be shared with third parties;[34] 71% of respondents reported that they were unaware that EU legislation, such as the DMA, may require search engines to share certain search data with competing providers.[35]

These findings provide important context specifically for Article 6(11). Unlike data portability under the GDPR or Article 6(9) of the DMA, the data sharing is neither initiated nor approved by the user, and the user has no means to opt out, short of no longer using the gatekeeper services. The legal standard for anonymisation, therefore, performs an important function. It must enable the objectives of Article 6(11) DMA to be achieved and at the same time ensure that the data made available cannot reasonably be linked back to identifiable individuals, consistent with a broader understanding of "anonymisation" and users' legitimate expectations regarding the treatment of their search history.

The consumer in brief:

- **Search is near-universal:** 90% use a search engine daily, up to 95% in Spain.
- **AI does not yet have the same reach:** for quick answers, 60% turn to search; 12% prefer chatbots.
- **More Sensitive questions go to search:** 59% often use search for sensitive topics, 37% use chatbots.
- **A strong expectation of confidentiality:** 66% expect search history to stay confidential;
- **Low Awareness:** 71% were unaware of the DMA sharing rule.

[34] EPPP DMA Awareness Survey, Q12 (n=3,045). *Q12. Before today, were you aware that under European Union (EU) regulations, such as the Digital Markets Act (DMA), internet search engines may be required to share user search data with competing companies?*

[35] EPPP DMA Awareness Survey, Q12 (n=3,045). 71% reported that they were not aware, before the survey, that EU regulations such as the DMA may require search engines to share user search data with competing companies; awareness was lowest in Slovakia (80% unaware) and highest in Ireland and Estonia (around 63% unaware).

IV. The Anonymisation Question at the Centre

1. The sensitivity and contextual nature of search query data

As indicated above, search query data can be personal in nature and even intimate. Some searches may also reveal special category data in the sense of Art. 9 GDPR; of course, many also do not. A single user's queries over a week may include a question of who painted the Mona Lisa, a recipe for apple cake, or the value of a certain used car; but it could also ask about specific medications, the symptoms of a suspected condition, a clinic's address, financial pressures, or considerations on held personal beliefs. The significance of search data for Article 6(11) DMA is also about what can be inferred from queries taken in combination.

Search data can support inferences about a person, and, combined with metadata (when a query was made, from where, on what device, in which language, in what sequence) and with other queries or auxiliary datasets a recipient already holds, can single an individual out and assemble a detailed profile. This is the "mosaic" quality of search data: individually innocuous points that, in combination, become identifying.

As indicated above, queries also frequently contain the personal data of third parties, such as a family member's name, a colleague's contact details or excerpts of tax filings, widening the set of people a dataset can be made to speak about. This is distinct from the anonymisation concerning the end user. A name appearing in a query is the third party's personal data and engages their rights, but it does not, on its own, make the user who entered the query identifiable. These are two separate questions, though both bear on how much of the data falls within the anonymisation context: a question of scope to which the operative text of Article 6(11), which speaks of "any… data that constitutes personal data," and Recital 61, which refers to end users, arguably give potentially different answers.[36]

2. The DMA–GDPR relationship in the context of anonymisation

How the DMA and the GDPR relate in law is foundational to this debate, and CIPL has examined the interplay at length.[37] Two points govern how we think about this interplay.

- **The DMA is not lex specialis to the GDPR.** The DMA is based solely on Article 114 TFEU, whose objective is the functioning of the internal market. It is not based on Article 16 TFEU, the specific Treaty legal basis for data protection. Under Article 114, the DMA cannot be regarded as regulating personal data processing as *lex specialis*. Both instruments apply "without prejudice"

[36]Article 6(11) DMA provides that "any… query, click and view data that constitutes personal data shall be anonymised," without limiting the obligation to end-user data, while Recital 61 refers to the personal data of end users. Under settled CJEU case law, a recital may aid interpretation but cannot restrict the scope of an operative provision (see, e.g., C-134/08, *Hauptzollamt Bremen v J.E. Tyson Parketthandel*, para 16). The relationship between the operative text and the recital is a live interpretive question that bears on how much data falls within the anonymisation duty.

[37]CIPL, *Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences*, May 2023; CIPL, *Response to the European Commission and EDPB Public Consultation on the Draft Joint Guidelines*, December 2025.

to each other,[38] and the Court has confirmed in *Malta v Commission* that where two EU acts of equal hierarchical value do not establish a relationship of priority, they must be applied compatibly to ensure a coherent interpretation.[39] The principle of sincere cooperation, reaffirmed by the *Bundeskartellamt*, extends that duty to the authorities responsible for enforcing each instrument.[40]

- **Implementation must not lower GDPR protection.** The interpretation of DMA obligations must not result in a lowering of the level of data protection and privacy afforded by the GDPR for the sake of DMA objectives. The GDPR is a fundamental rights instrument anchored in the EU Charter;[41] the DMA is a market-regulation instrument focused on contestability and fairness. Where they overlap, the GDPR's foundational role must be preserved. A useful comparator is the Data Act, whose Article 1(5) expressly preserves the application of EU data protection law in the data-sharing obligations it creates.[42] Article 6(11) DMA contains no equivalent.

It follows that the term "anonymised" in Article 6(11), where it concerns personal or sensitive data in the sense of the GDPR, should ultimately carry the meaning the term is given in the GDPR context. A different, DMA-specific meaning would place data shared under Article 6(11) outside the GDPR's protections even where, in the recipient's hands, it may still carry a level of potential for identification, which would deem it at most pseudonymised. This would result in the same data being considered "anonymised" for the DMA and yet personal under the GDPR. The Joint Guidelines of the Commission and the EDPB, and the joint EDPB–EDPS opinion on the Digital Omnibus, accept that technical anonymisation measures may be complemented by contractual and organisational safeguards on recipients, such as prohibitions on re-identification, purpose limitation and security obligations. That layered approach can be a legitimate part of the architecture, and CIPL has long supported pairing robust technical measures with strong organisational and contractual safeguards.

As mentioned above, however, the question it raises is one of balance. Where the technical de-identification step has already reduced identifiability sufficiently, contractual and organisational measures properly reinforce that outcome and address minimal residual risk. Where, by contrast, the recipient's own application of those measures does the decisive work, it remains a question whether that data is closer to being pseudonymised or anonymised. This question should be resolved by data

[38]DMA Recital 12: "This Regulation should also apply without prejudice to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation, in particular Regulations (EU) 2016/679 and (EU) 2019/1150 of the European Parliament and of the Council and a Regulation on a single market for digital services, and Directives 2002/58/EC, 2005/29/EC, 2010/13/EU, (EU) 2015/2366, (EU) 2019/790 and (EU) 2019/882 of the European Parliament and of the Council, and Council Directive 93/13/EEC, as well as national rules aimed at enforcing or implementing those Union legal acts.."
[39]Judgment of 12 May 2021, *Republic of Malta v European Commission*, T-653/16, paragraph 137 (where two EU acts of equal hierarchical value do not establish a relationship of priority, they must be applied compatibly to ensure a coherent interpretation).
[40]Judgment of 4 July 2023, *Meta Platforms Inc. v Bundeskartellamt*, C-252/21 (sincere cooperation between competition authorities and data protection authorities).
[41]Charter of Fundamental Rights of the European Union, Articles 7 and 8.
[42]Regulation (EU) 2023/2854 (Data Act), Article 1(5), which preserves the application of EU data protection law in the data-sharing obligations the Data Act creates. Article 6(11) DMA contains no equivalent express preservation, but the absence of such a clause cannot be read to displace the legal position that the two instruments apply compatibly.

protection authorities and the Commission in cooperation, involving technical experts. This may ultimately be a question for the legislator, though, as proposed in the Digital Omnibus or an implementing act as proposed by the Commission to ensure a unified approach. However, the resulting standard should then be applicable beyond the DMA, in the context of the GDPR and across the digital acquis.

Our survey asked how respondents thought about their search data shared with third parties when it was in fact anonymised first.[43] Respondents were split almost evenly (35% find acceptable, 36% unacceptable). However, half of all respondents (50%) said they believed it likely that anonymised search data could be re-identified and linked back to them, with only 16% considering re-identification unlikely.[44] These figures record public sentiment, not a technical expert's assessment, of course, and nothing in their views settles the legal question of whether a given construct meets the GDPR's standard.[45] However, if Article 6(11) intends to enable contestability of the market in a way that ultimately benefits users, users should be brought on the journey.

V. TOWARD A SINGLE, CONSISTENT STANDARD

As the term "anonymised" in the context of Article 6(11) must align with the GDPR, the question becomes what that requires in practice, and how the obligation can be implemented so that it advances contestability while ensuring appropriate protection of the individual. The data sharing obligation is not in question, nor should anonymisation require emptying the dataset of every unique or competitively valuable query, which would defeat the obligation's purpose. CIPL has long argued that a GDPR-consistent standard should not be a maximalist one; re-identification should be made unlikely by the means reasonably likely to be used, not impossible in the abstract.

1. A relative, risk-based reading

A GDPR-consistent reading of DMA Article 6(11) has two components, each drawn directly from the GDPR's own framework.

- **Identifiability is assessed by reference to the means reasonably likely to be used, including by the recipient.** This is the Recital 26 GDPR standard confirmed by SRB.[46] It is context-dependent:

[43] EPPP DMA Awareness Survey, Q14. (n=3,045). *Q14. If an internet search engine removed your personal details, how acceptable would you find it if competing companies used your search data to build their services? T2B = Completely acceptable + Somewhat acceptable, B2B = Completely unacceptable + Somewhat unacceptable.*

[44] EPPP DMA Awareness Survey, Q15 (n=3,045). 50% consider it likely that anonymised search data could be re-identified and linked back to them (highest in Estonia at 56%, lowest in Slovakia at 39%); 16% consider re-identification unlikely. *Q15. If search engines were legally required to share anonymised search data with other companies, how likely or unlikely do you think it is that this data could be re-identified and linked back to you? T2B = Very likely + Somewhat likely, B2B = Very unlikely + Somewhat unlikely*

[45] It may suggest that more public education on data protection and privacy standards in the European Union would be of benefit to its citizens.

[46] GDPR Recital 26: 'To determine whether a natural person is identifiable, account should be taken of 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'; Judgment of 7 March 2025, Single Resolution Board v European Data

the same dataset may be anonymised for one recipient and personal data for another. For Article 6(11), this means assessing the actual recipient profile, auxiliary data, and capabilities, not a generic 'third party'

- **Technical measures should form the foundation with governance measures reinforcing them.** There is a difference in kind between measures that change what the data is and measures that govern what a recipient may do with it.[47] CIPL has consistently supported pairing robust technical measures, including privacy-enhancing technologies such as differential privacy, synthetic data and generalisation, with organisational and contractual safeguards, and recipient governance is a valuable and appropriate part of the Article 6(11) architecture. Where the technical de-identification step has already sufficiently reduced identifiability, contractual safeguards properly reinforce that outcome and guard against downstream misuse. Where, by contrast, those safeguards are relied on to bridge a technical gap, the data may be closer to pseudonymisation under safeguards than anonymisation. Distinguishing the two is the relative, recipient-specific assessment that *SRB* calls for.[48]

The Commission's proposed measures have received extensive input through the consultation process,[49] and data protection specialists and experts have raised their concerns.[50] Whether the proposed technical solution can sufficiently reconcile anonymity and utility with the granularity the obligation contemplates is partly a technical question, but it should not be left to case-by-case determination by individual authorities alone. Any anonymisation standard accepted in the DMA context, including as to additional safeguards, should be applied consistently across the GDPR, the DMA and the wider digital acquis going forward. That standard should build on the Court's reasoning in SRB, with its relative, risk-based approach to identifiability, and on the ongoing institutional discussion, rather than allowing "anonymised" to take on a bespoke meaning in the DMA-enforcement context.

Protection Supervisor, C-413/23 P (CJEU on the relative concept of personal data and the assessment of identifiability from the perspective of the recipient).

[47] The European Data Protection Board in its draft Guidelines 02/2026 on Anonymisation confirms this by stating that: (para 34) "*A prohibition set out in a contract (even if it is legally binding upon its parties) should not be treated as a prohibition by law. While contractual terms may have an effect on the means reasonably likely to be used, they should only be used to complement technical measures, and it is important to carefully consider the actual strength of their effect. Among other things, the measures should be reliable, verifiable and enforceable, bearing in mind that contractual measures can typically be subject to revision, or may even be disregarded entirely by the parties*."

[48] European Commission, *DMA.100209 – SP – Alphabet – Article 6(11) Google Search Data Sharing: Case Summary*, 16 April 2026, p. 2 (technical measures reduce the likelihood of re-identification of end users to a "residual level"; contractual measures "complement the technical measures to further reduce the likelihood of re-identification of end users to an insignificant level").

[49] We applaud the Commission for engaging in this valuable stakeholder process.

[50] For example, please see Mark Leiser (https://substack.com/home/post/p-202400288); International Centre for Law & economics (https://laweconcenter.org/resources/icle-comments-to-the-european-commission-on-alphabets-article-611-dma-obligations/); European Centre for International Political Economy (https://ecipe.org/insights/dma-proceedings-against-google/).

2. The trust gap and implications for the data sharing provisions

A final section of CIPL's consumer survey wanted to know how respondents considered agency over their search data. In an interesting contrast to respondents' assumption of confidentiality of their search data, 45% of respondents feel they have little or no control over how their search data is used by search engines.[51]

Given a choice between the most commonly known safeguards they would like to see in the DMA context, respondents ranked these as follows: the right to say no (51%), active consent (41%), data deletion (37%), clear notification (31%), strict usage limits (27%), a technical guarantee (24%) and an isolation guarantee (21%).[52] The three most-wanted safeguards are, in substance, the GDPR's own (the ability to refuse, to consent meaningfully, and to have one's data erased) and therefore likely the most familiar, while the more technical options ranked lower. The by country detail shows that in Germany, active consent (49%) was nearly as important as the right to refuse, and in Spain and France, data deletion was a particularly high priority (around 39%)

The safeguards consumers want most (if sharing is mandated)

- **The right to say no:** 51%
- **Active consent:** 41% (49% in Germany)
- **Data deletion:** 37% (around 39% in Spain and France)
- **Clear notification:** 31%
- **Strict usage limits:** 27%
- **Technical guarantee:** 24%
- **Isolation guarantee:** 21%
- *The favoured safeguards mirror the GDPR rights*

With the structure of Article 6(11) as it stands, transparency is the most tangible way to close the existing trust gap. User-facing information should be built into the process.

[51]EPPP DMA Awareness Survey, Q16_1 and Q16_2 (n=3,045). 45% feel they have little or no control over how their search data is used by internet search engines; the figure rises to 50% for AI chatbots. *Q16_1. To what extent do you feel you have control over how your search history (search data) is used by internet search engines or AI chatbots? T2B = I feel I have complete control + I feel I have a lot of control, B2B = I feel I have no control at all + I feel I have very little control; Q16_2. To what extent do you feel you have control over how your search history (search data) is used by internet search engines or AI chatbots? T2B = I feel I have complete control + I feel I have a lot of control, B2B = = I feel I have no control at all + I feel I have very little control*.

[52]EPPP DMA Awareness Survey, Q17 (n=3,045). Asked which privacy protection measure would matter most if data sharing were mandated by law, respondents selected: the right to say no 51%; active consent 41%; data deletion 37%; clear notification 31%; strict usage limits 27%; technical guarantee 24%; isolation guarantee 21%. In Germany, active consent (49%) was nearly as important as the right to refuse; in Spain and France, data deletion was a particularly high priority (around 39%); *Q17. If the law were to mandate the sharing of search data, which of the following privacy protection measures would you consider most important?*

A single, GDPR-consistent standard, supported by governed recipients and genuine transparency to users, is the configuration most likely to deliver contestability without reducing the trust on which both the DMA and the GDPR ultimately depend.

Respondents were also presented with two statements describing competing priorities (one prioritising the security of their data and privacy, the other prioritising a system that supports new businesses to enter the market and compete), anchored at opposite ends of a five-point scale. Unsurprisingly, the result leaned heavily towards privacy: 42% placed themselves at the strongest privacy position against just 8% at the strongest competition position, and on a top-two-box basis, 62% favoured the privacy framing against 16% for the competition framing.[53] The privacy preference was strongest in Estonia (50% at the highest privacy score) and Spain (45%). People will choose what is most familiar to them.

Of course, users benefit from both: trusted digital services and a market that offers choices. The implication is therefore not that contestability should yield to privacy or vice versa. But users must be brought onto the journey to instil trust in the digital market and the legitimate aims of the DMA. The task the evidence sets for policymakers is to design for the "both," not to adjudicate the "either."

When asked to choose, Europeans lean towards privacy

- **42%** placed themselves at the strongest privacy position; only **8%** at the strongest competition position.
- **62% vs 16%** favoured the privacy framing over the competition framing on a top-two-box basis.
- **Strongest in Estonia (50%) and Spain (45%);** no market reversed the ordering.
- *Privacy-versus-competition should not be the choice: most users want both. The design task is the "both," not the "either."*

VI. RECOMMENDATIONS

CIPL supports the objective of Article 6(11) and the sharing of search data it mandates. The recommendations below set out how to give effect to that obligation so that it advances contestability while resting on a single, GDPR-consistent standard of anonymisation.

1. **Implement Article 6(11) on a single, GDPR-consistent standard of anonymisation that applies consistently across the digital acquis.**

The term "anonymised" in Article 6(11) DMA should carry the meaning it has in the GDPR context: whether identification of a natural person is reasonably possible, taking into account all the means

[53]EPPP DMA Awareness Survey, Q13 (n=3,045). On a five-point scale anchored by a privacy statement and a market-competition statement, 42% selected the strongest privacy position and 8% the strongest competition position; on a top-two-box basis, 62% leaned to the privacy framing and 16% to the competition framing. As discussed below, a forced choice of this kind is a polarising instrument and is read here with corresponding caution.

reasonably likely to be used (Recital 26 GDPR), as confirmed by the Court of Justice in *SRB* and continues to be developed in the EDPB's guidance (and ultimately as part of the Digital Omnibus). A bespoke, DMA-specific application, whether more permissive or more restrictive than the GDPR's, would create two standards for a single concept, one calibrated to the internal market and one to fundamental rights, generating legal uncertainty and running contrary to the simplification objectives across the digital acquis. The standard settled in the Article 6(11) context should be applicable consistently across the GDPR and the digital acquis.

2. **Apply a relative, risk-based assessment.**

Consistency with the GDPR does not mean importing a zero-risk standard. Following *SRB*, identifiability is assessed by reference to the means reasonably likely to be used by the actual recipient, its capabilities, auxiliary data and context, not by hypothetical, unlimited adversaries. Re-identification should be made unlikely, not impossible in the abstract.

3. **Anchor anonymisation in robust technical measures, with contractual and organisational safeguards reinforcing them.**

There is a difference in kind between measures that change what the data is and measures that govern what a recipient may do with it. Technical de-identification, including privacy-enhancing technologies such as differential privacy, synthetic data generation and generalisation, should carry the decisive work of reducing identifiability. Contractual and organisational safeguards — prohibitions on re-identification and linkage, purpose limitation, retention limits, onward-sharing restrictions and independent audit — are valuable accountability instruments that CIPL has long supported, and they properly reinforce a technically sound outcome and guard against downstream misuse. Whether proposed measures strike the right balance towards an acceptable standard should be determined by the Commission and data protection authorities together, with the involvement of technical experts; and the balance accepted there should then hold reciprocally in the GDPR context.

4. **Coordinate the three workstreams shaping "anonymised" to avoid fragmentation.**

The meaning of anonymisation is currently being determined administratively (DMA.100209), interpreted judicially and in draft EDPB guidance, and reshaped legislatively through the Digital Omnibus — in parallel and not always in step. Regulatory cooperation between the Commission, the EDPB and national DPAs should ensure that DPA expertise is reflected in binding specification measures. If coordination between the institutions cannot deliver a single standard, resolving the question may ultimately fall to the legislator — through the Digital Omnibus or an implementing act — to prevent divergent understanding and standards from consolidating. Regardless, meaningful outcomes will require strong stakeholder involvement on both the sharing and the receiving side of Article 6(11).

5. **Consider the end user in the implementation of Article 6(11), and bring users on the journey.**

The individuals whose data is shared are not a party to the regulatory dialogue, and the sharing in the context of Article 6(11) is neither initiated nor approved by the user. The CIPL–EPPP six-market survey shows a discrepancy: 66% of Europeans expect their search history to remain confidential, 71% are unaware of the DMA sharing obligation, half believe anonymised data could be re-identified and look for agency. Within the structure of Article 6(11) as it stands, transparency is the most tangible means of closing that trust gap. As Article 6(11) is implemented, consideration should be given to measures by stakeholders that promote greater clarity around how users' search interactions relate to the data-sharing regime, including accessible information about third parties that may be granted access.

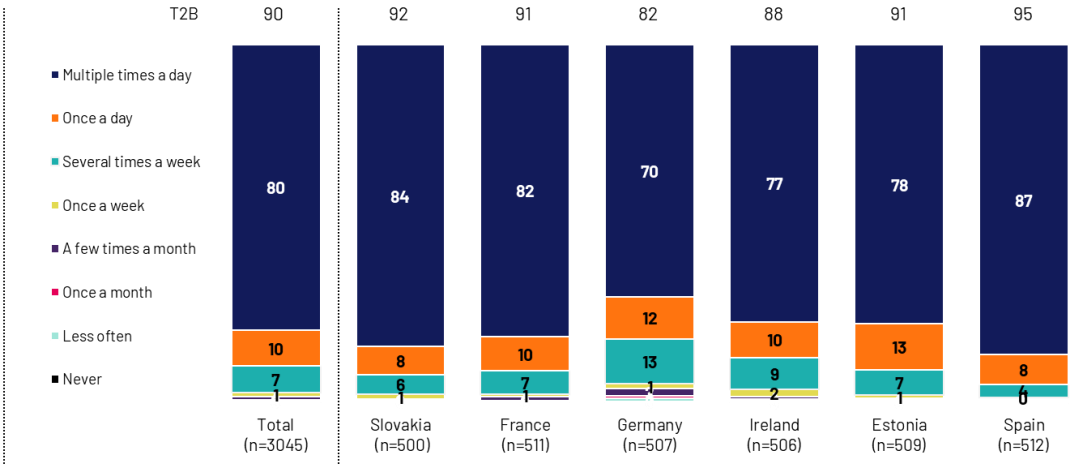
ABOUT CIPL

The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

VII. ANNEX

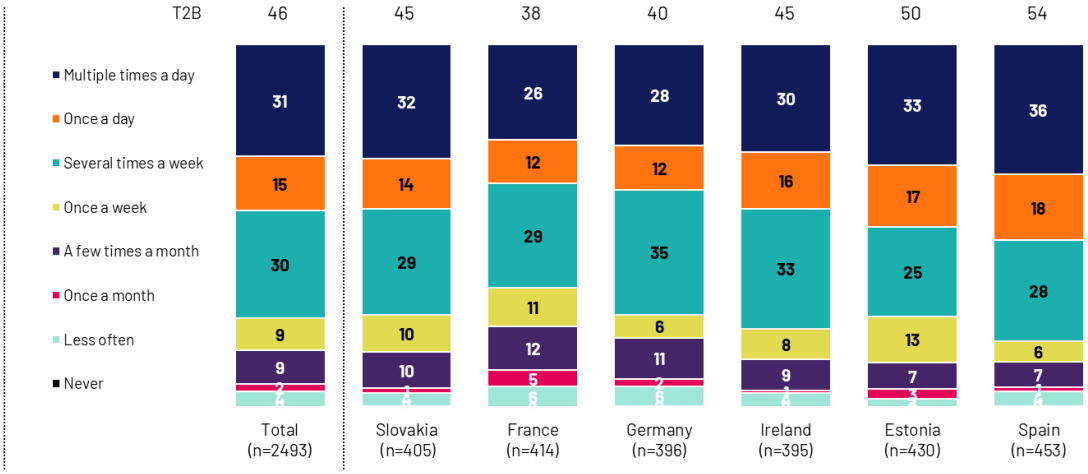
1. How often do respondents use internet search engines?

Q2. How often do you typically use internet search engines? An internet search engine is an online service (e.g. Google, Bing, etc.) where you can enter keywords or questions to find information on the internet. As a result, it shows you a list of relevant links.T2B = Multiple times a day + Once a day.



2. How often do respondents use AI chatbots?

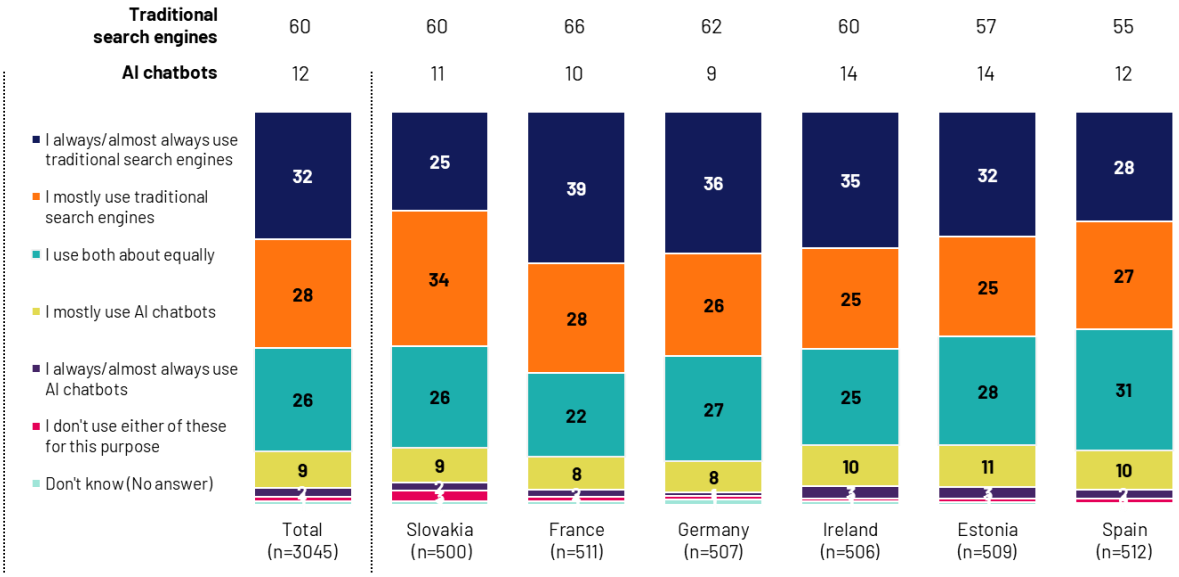
Q4. How often do you typically use generative artificial intelligence tools - AI chatbots (e.g. ChatGPT, Gemini, etc.)? T2B = Multiple times a day + Once a day.



Methodology. The CIPL–EPPP DMA Awareness Survey was conducted by Ipsos using computer-assisted self-interviewing (CASI) via the Ipsos online panel, with a quantitative questionnaire of approximately ten minutes. Fieldwork ran from 22 to 29 May 2026 across six EU markets — Slovakia, Germany, France, Ireland, Estonia and Spain — with a target of 500 respondents per market (total n=3,045). The sample in each market is representative of the online population aged 18 and over, with quotas set by age, region and gender. Figures throughout are reported as percentages. "T2B" refers to the top-two-box values on a response scale and "B2B" to the bottom-two-box values.

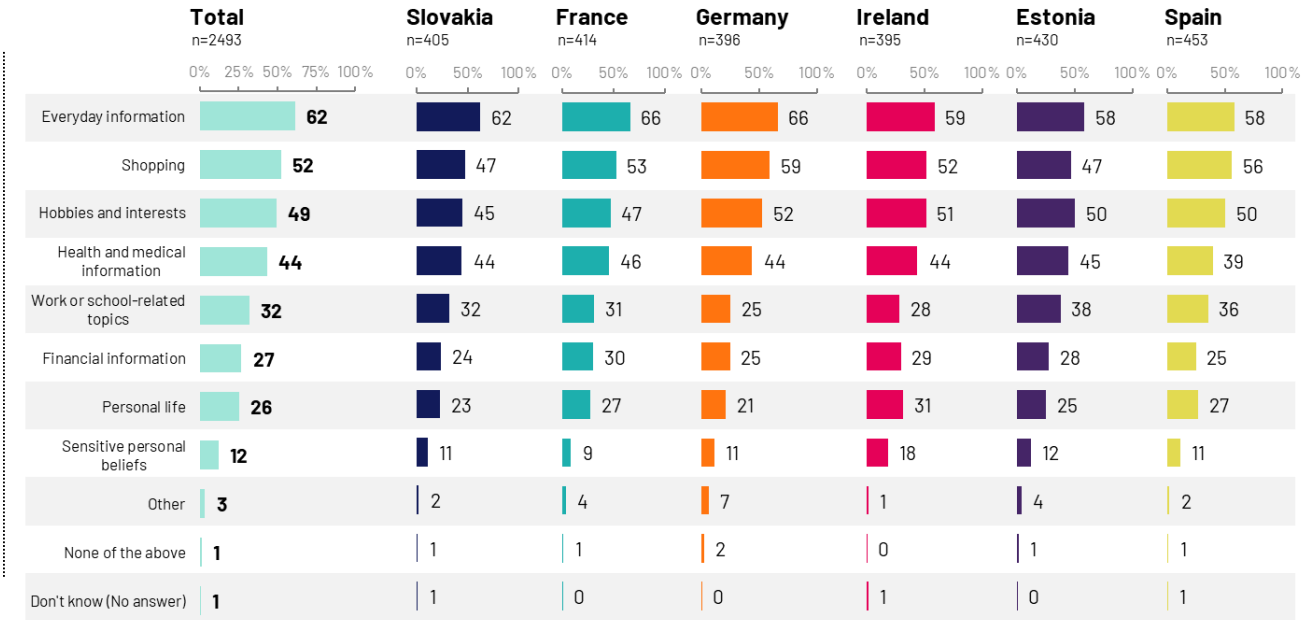
3. Do respondents use traditional search engines or AI chatbots for quick answers?

Q5b. Would you say that when searching for information, or getting quick answers to questions, you more often use traditional internet search engines (e.g. Google, Bing, etc.), or AI chatbots (e.g. Gemini, ChatGPT, etc.)?



4. What have respondents been searching for?

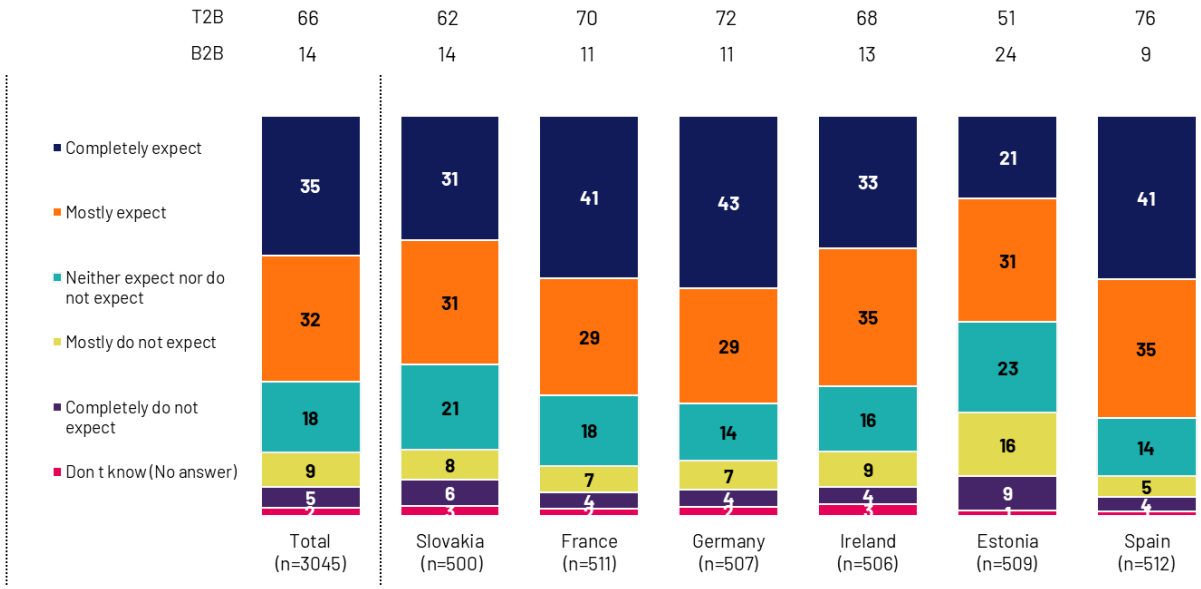
Q7: Thinking about the topics you have searched for online in the past month, which of the following areas do these topics fall into? Please select all that apply.



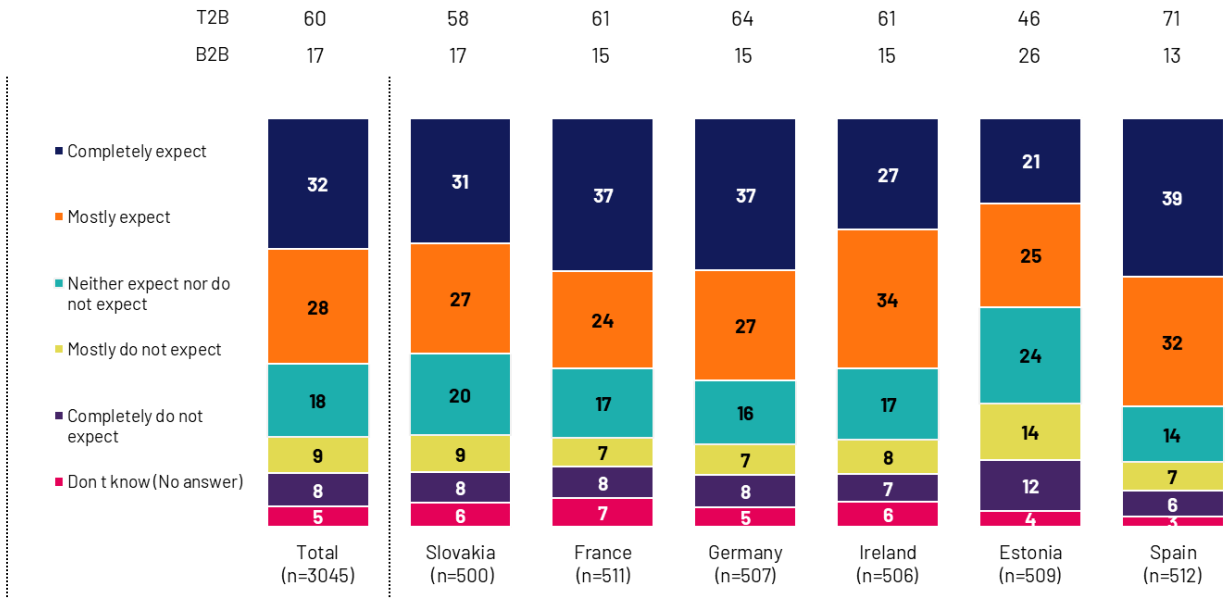
5. Expectations of confidentiality

Q7a: When you use an internet search engine or an AI chatbot, to what extent do you expect your individual search history to remain confidential between you and the providers of the service? T2B = Completely expect + Mostly expect, B2B = Completely do not expect + Mostly do not expect

Search engines:

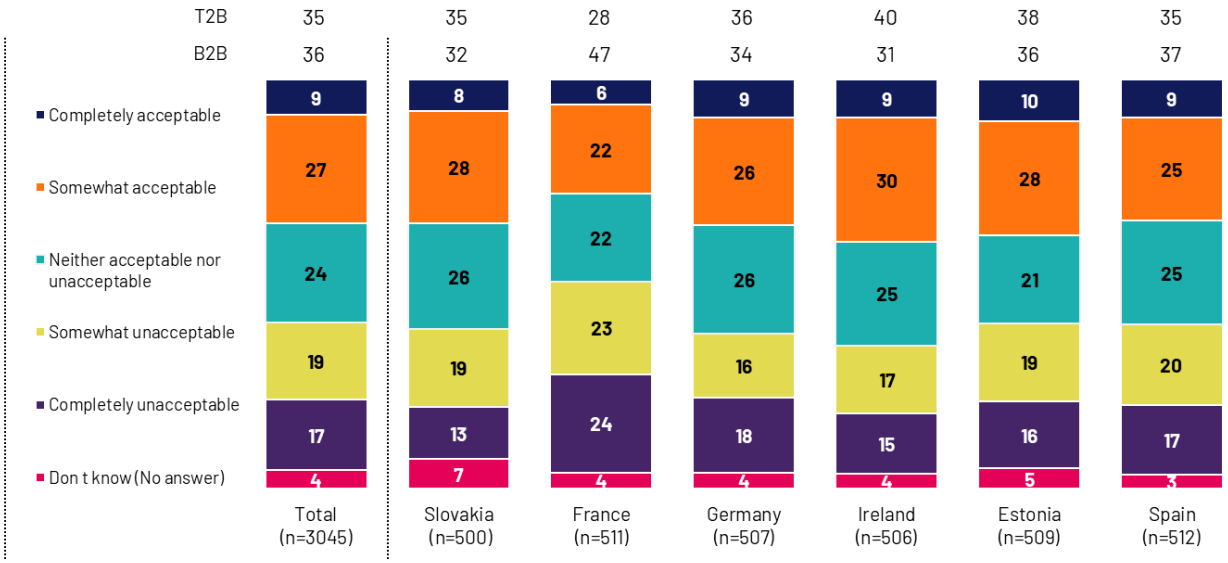


AI chatbots:



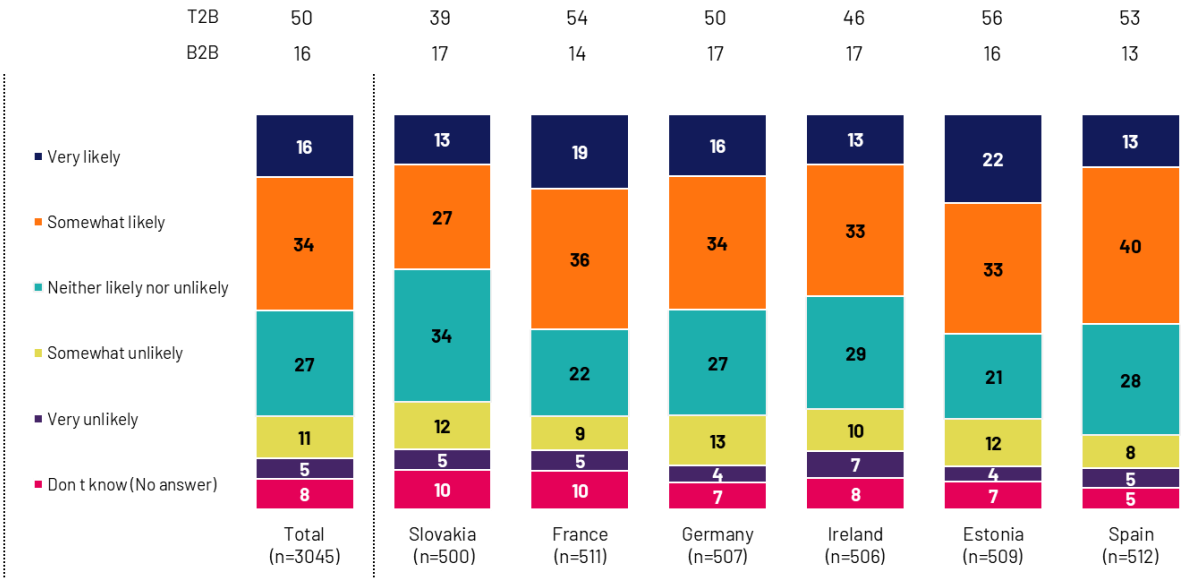
6. Acceptability of sharing search data with removed personal details

Q14: If an internet search engine removed your personal details, how acceptable would you find it if competing companies used your search data to build their services? T2B = Completely acceptable + Somewhat acceptable, B2B = Completely unacceptable + Somewhat unacceptable



7. Likelihood of data re-identification

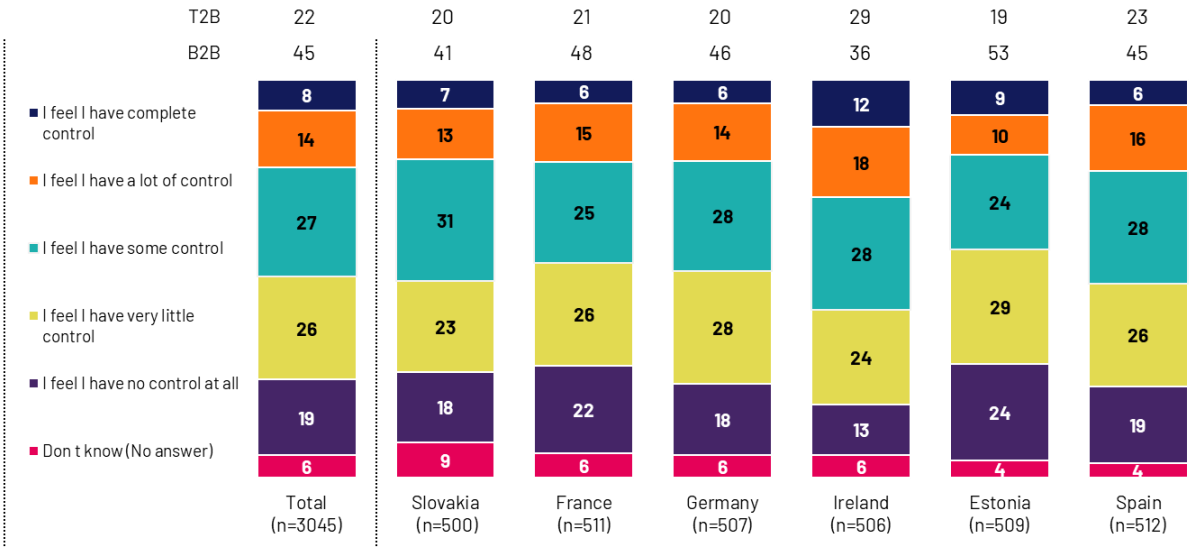
Q15. If search engines were legally required to share anonymised search data with other companies, how likely or unlikely do you think it is that this data could be re-identified and linked back to you? T2B = Very likely + Somewhat likely, B2B = Very unlikely + Somewhat unlikely



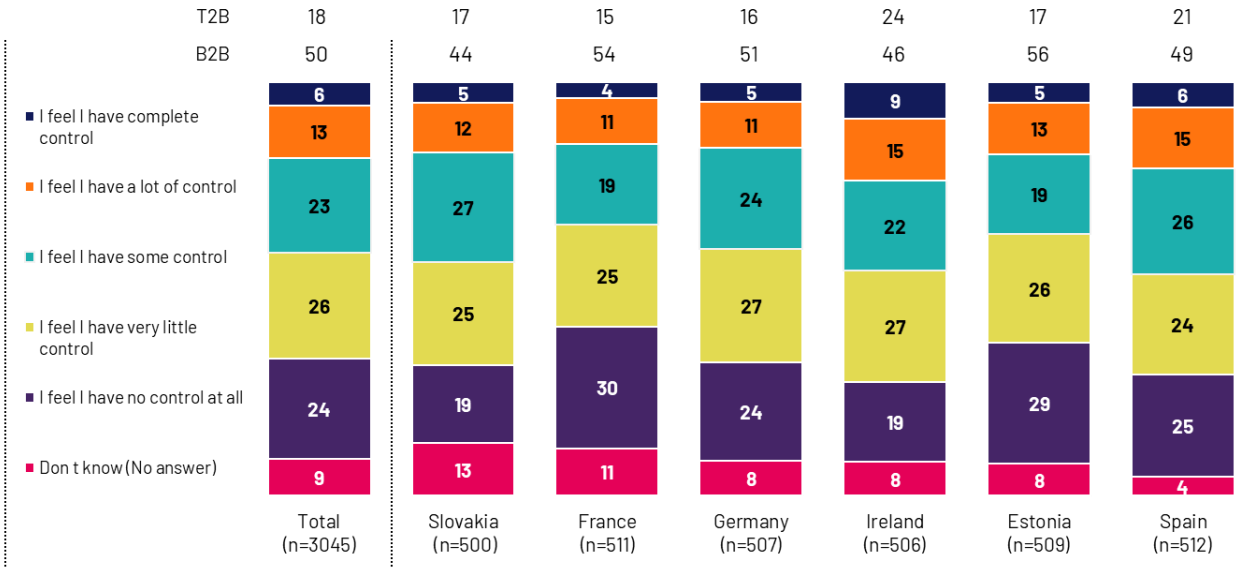
8. Perceived Control Over Search Data

Q16_1. To what extent do you feel you have control over how your search history (search data) is used by internet search engines or AI chatbots? T2B = I feel I have complete control + I feel I have a lot of control, B2B = I feel I have no control at all + I feel I have very little control

Search engines:

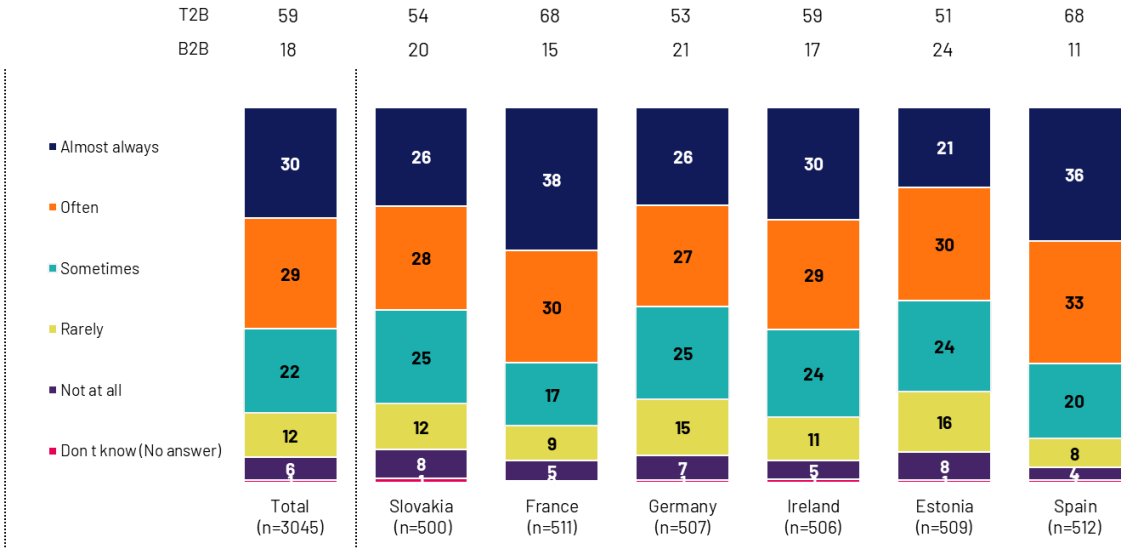


AI chatbots:



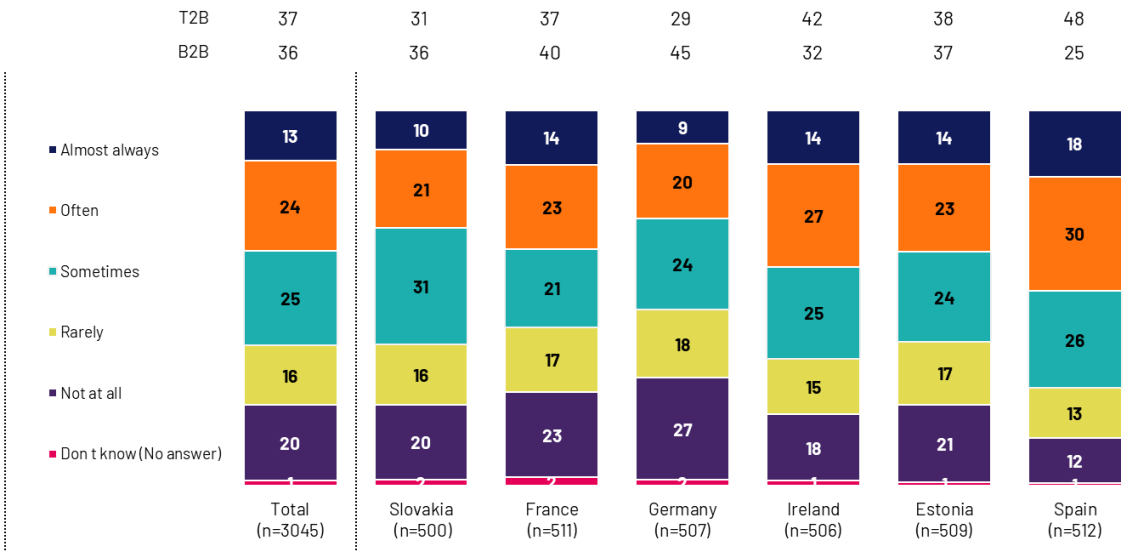
9. Use of Search Engines for Sensitive Topics

6_1. To what extent do you use internet search engines or AI chatbots to ask questions about sensitive or intimate topics for you (such as health, finances, personal life, or your personal beliefs)? T2B = Almost always + Often, B2B = Rarely + Not at all



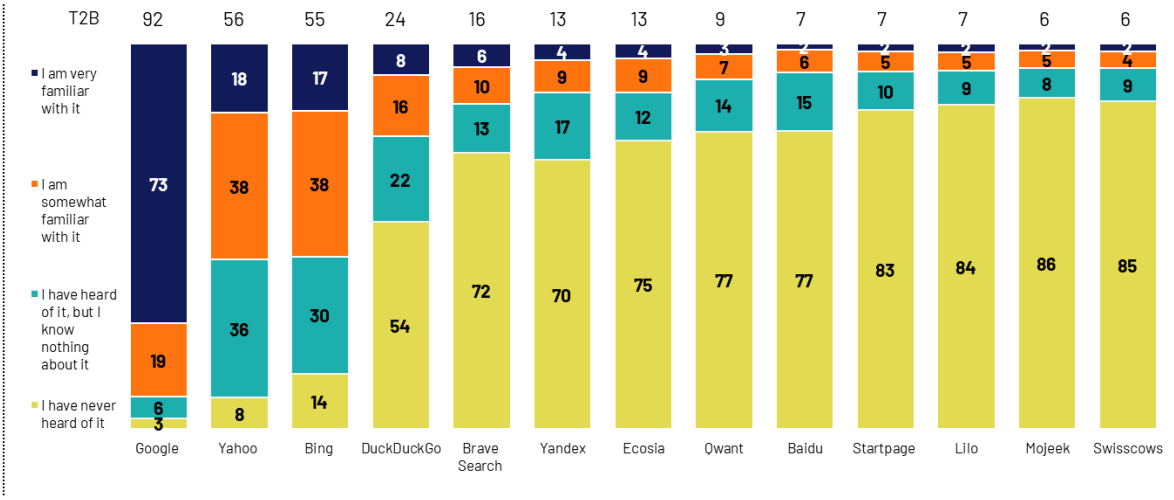
10. Use of AI chatbots for Sensitive Topics

6_2. To what extent do you use internet search engines or AI chatbots to ask questions about sensitive or intimate topics for you (such as health, finances, personal life, or your personal beliefs)? T2B = Almost always + Often, B2B = Rarely + Not at all



11. Familiarity with Internet Search Engines

Q8. To what extent are you familiar with the following internet search engines? T2B = I am very familiar with it + I am somewhat familiar with it. n=3045



12. Familiarity with AI chatbots

Q10. To what extent are you familiar with the following AI chatbots?T2B = I am very familiar with it + I am somewhat familiar with it, n=3045