Introduction:

The European Union's ambition to create a harmonized, competitive, and rights-respecting digital single market can be advanced by both the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR). Ensuring these two landmark regulations work coherently together is crucial for providing legal certainty, fostering innovation, and protecting users. The draft joint guidelines from the European Commission and the European Data Protection Board (EDPB) represent an important step in clarifying this interplay.

AmCham Poland aims to provide insights grounded in operational realities to help ensure the final guidance achieves its objectives without creating unintended friction that could come to the detriment of users' privacy and security, impede innovation, undermine the effectiveness of either regulatory framework or harm user experience

General comments:

In our opinion, some of the underlying assumptions of the guidelines are misguided and pose a threat to the objectives of the GDPR and DMA:

1) The Guidelines prevent designated companies from protecting EU customers' personal data by mischaracterizing essential security measures as prohibited barriers. Companies must be able to carry out their safety and security checks of third parties to ensure that EU citizens' intimate personal information is ported in a responsible fashion. Instead of sacrificing these security standards, the Guidelines should expressly allow for such controls and should set a common standard for these safety and security checks across designated companies, as they have been called to do. Without these controls, nefarious actors might gain access to EU citizens' data. In fact, designated companies have in the interim seen many nefarious applicants including overseas actors from highrisk jurisdictions and entities lacking the basic privacy compliance frameworks.

2) The Guidelines might undermine efforts to protect EU customers and citizens and sacrifice their fundamental rights by subordinating data privacy to the portability obligation with uncertain benefit to customers and impact on contestability. In our opinion, portability should not compromise data minimisation. In this regard, the guidelines appear to endorse a GDPR trade-off in favor of the DMA. Fundamentally, from a privacy perspective, laws should not force companies to collect new data, resulting in lower privacy protections for users.

3) More generally, the Guidelines seem to imply that GPDR (its rights and obligations; and even arguably privacy as a fundamental right) is secondary to DMA and designated companies should override GDPR obligations and protections of EU customers to comply with competing obligations.

4) The Guidelines suggest departure from the DMA opt-in consent for data sharing between service to a per-purpose opt-in. Imposing opt-in consent per specific purpose, including service development, is disproportionate in view of the legislative objective of Article 5(2): it harms innovation without a commensurate

privacy benefit, particularly where techniques exist to minimise the use of personal data and offering even more granular consent prompts on a per-service basis creates consent fatigue (as evidenced in the cookies context).

5) Undue restriction of design choices that do not impact customer behaviours should be avoided. While the DMA requires user consent in accordance with GDPR standards, some examples in the Guidelines seem to go against established design choices without clear justification. For example, the Guidelines suggest that color contrast in consent buttons could be considered misleading or nudging, yet color contrast enhances visibility, accessibility, and transparency of choice.

6) Guidelines should recognise gatekeepers' ability to differentiate their platforms on the level of privacy protections afforded to users. They should therefore allow gatekeepers to place appropriate privacy-enhancing safeguards on all apps distributed on a gatekeepers' platform, including via alternative marketplaces.

7) Some provisions of the Guidelines seem to be contradictory or set a double-standard depending on the provision. First, designated companies are considered data controllers under the GDPR, as providers of operating systems and app developers, when complying with the distribution of apps and app stores obligation in Article 6(4) (para. 92). They are required to comply with Article 6(4) while also ensuring their compliance with the GDPR (para. 88). On the other hand, designated companies are exempted from their GDPR obligations when porting data to customers and third parties under the Portability obligation. Second, the Guidelines highlight the requirement of effective anonymization under Article 6(11) for search-data sharing to protect end users' GDPR rights. By contrast, under Article 6(9) the Guidelines do not endorse designated companies to apply appropriate third-party authorization or vetting mechanisms to mitigate GDPR compliance risk. Instead, the Guidelines should arrive at a single standard allowing designated companies to vet third parties appropriately in compliance with the GDPR while effectively complying with the portability obligation.

8) The Guidelines create contradictions between established GDPR notions versus DMA. For example, the Guidelines (paras. 25-27) take the position that the DMA allows suppressing functionalities when consent is withheld as long as the designated company notifies the user. The GDPR position (para. 34) is that refusing consent must come without detriment and negative consequences. This creates a direct contradiction: any service degradation (even if due to technical necessity from lack of data) could be seen as "detriment" under GDPR as per the Guidelines, making it impossible for companies to comply with both requirements simultaneously. The Guidelines state cross-use of personal data must be "strictly necessary" for interconnected functionality under the DMA (para. 69), applying a very narrow interpretation not found in the DMA text itself. However, the Guidelines take a broader view under GDPR, suggesting gatekeepers can rely on legitimate interests rather than strict necessity (para. 74). This creates particular confusion for advertising services, where the Guidelines simultaneously suggest that processing for online advertising

"cannot be seen as strictly necessary" (para. 73) yet may be permissible under GDPR legitimate interest grounds.

9) The Guidelines contradict established data protection principles in the Data Act. In particular, the Guidelines' interpretation (paras. 105-106) that DMA Article 6(9) data portability operates independently of GDPR compliance and relieves gatekeepers of responsibility for third-party data protection compliance directly conflicts with how similar data portability rights are treated in the Data Act (Regulation 2023/2584), where GDPR primacy is explicitly preserved (Article 1(5)). The EC Data Act FAQs reinforce that in data sharing scenarios between controllers, each must demonstrate GDPR compliance under the accountability principle. The Guidelines' departure from this established principle in the DMA context creates an unjustified dual standard of privacy protection - where a user's personal data receives different levels of protection depending on which EU instrument enables the sharing.

Specific comments:

Article 5(2)

The Guidelines seeks to ensure users have genuine, GDPR-compliant choices regarding data combination and cross-use. An overly broad or rigid interpretation of Art. 5(2) obligations—particularly one that mandates disruptive, purpose-specific choice screens—will bombard users, leading to significant product degradation,consumer harm and undermining meaningful consent.

1) Consumer Fatigue & "Choice Overload": Early data on the DMA's implementation already reveals significant consumer frustration. 39% of users report needing more steps for tasks that were once simple, and around one-third find their digital experience "less seamless and more confusing". This aligns with known "consent fatigue". Bombarding users with excessive, ill-timed prompts does not lead to informed decisions; it leads to confusion and arbitrary clicks, degrading the seamless experience they expect.

2) Erosion of Trust & Utility: This friction is especially counter-productive given the "Awareness Gap"—with 80% of consumers unfamiliar with the DMA , they experience these new hurdles as "pure friction without context". When core product functionalities are fragmented by constant interruptions, the service becomes less useful. This erodes trust and frustrates the user, rather than empowering them.

3) Counter-Productive to Privacy: This model of overwhelming users with low-value choices is counter-productive. It trains users to click through prompts just to get to the service they want, which can undermine the effectiveness of critical privacy and security warnings. It could also inadvertently run counter to the GDPR’s own principles of clarity and user-friendliness. This is particularly problematic when data shows consumers already demonstrate a strong preference for free, ad-supported services and only a "single-digit minority" are willing to pay for privacy-centric alternatives.

4) Opt-in consent for service development: Imposing this obligation is disproportionate in view of the legislative objective of Article 5(2): it harms innovation without a commensurate privacy benefit, particularly where techniques exist to minimise the use of personal data and offering even more granular consent prompts on a per-service basis creates consent fatigue (as evidenced in the cookies context). There is also no positive impact on contestability, including in AI development. As highlighted in the Draghi Report, the EU's strategic focus on AI development requires cross-industry coordination and data sharing to accelerate AI integration across key European industries. The Guidelines' restrictive approach could undermine the EU's ability to develop competitive AI capabilities, ultimately harming innovation.

5) Cross-service data sharing: The DMA regulates data sharing between services, but the Guidelines attempt to rewrite this into a more burdensome per-purpose consent system (paras. 31, 63). This overreach creates practical problems that the EDPB has itself recognized. In its letter to the Commission on its Cookie Pledge initiative (which was developed in response to concerns regarding cookie fatigue), the EDPB recognized that overly technical and lengthy descriptions render an informed choice complex, cumbersome and de facto ineffective. The Commission has also itself has acknowledged these issues in the ePrivacy context in September 2025, noting that "users are confronted with repetitive consent requests and non-transparent cookie banners, which make it difficult to understand how their data is used and in practice deprive them of a genuinely informed choice."

Article 6(7)

The omission of Article 6.7. from the Guidelines is concerning. Privacy and security considerations are frequently discussed in relation to interoperability and should be addressed in the Guidelines. Specifically the Guidelines should:

1) Recognise the privacy-related considerations should form part of the assessment of the "integrity of the operating system" under Article 6.7.

2) Stress the need for the EDPB and national protection supervisory authorities to be involved when gatekeepers' compliance with Article 6.7. carries the risk of undermining users' privacy rights and the GDPR

Article 6(9)

While extending data portability rights beyond the GDPR baseline can empower users, the draft Guidelines' expansion to include potentially vast 'generated' data, on-device data raises significant technical feasibility and privacy concerns. Requirements for "indefinite" continuous access and overly prescriptive reminder rules also require reconsideration for practicality and user experience.

1) Scope Expansion Challenges: Including data "generated through activity" (beyond data "provided by" the user significantly broadens the scope compared to GDPR Art. 20. Clarity is needed on what this encompasses, particularly

excluding genuinely inferred or derived data created by the gatekeeper. Mandating portability for on-device data presents substantial technical hurdles and security risks, potentially requiring entirely new, complex transfer mechanisms outside existing secure cloud infrastructures. Similarly, including personal data of other individuals within a user's portability request creates significant privacy conflicts and technical difficulties in segregation or obtaining consent.

2) Continuous and Real-Time Access: Providing "continuous and real-time access," especially "indefinitely," requires clarification. While ongoing access via APIs is valuable, truly real-time, indefinite synchronization for potentially massive datasets presents major technical, resource security challenges. Continuous, indefinite access tends to be a leading cause of major data breaches as it allows users and applications to accumulate more access than they actually need over time. Such compromised accounts with standing permissions can be exploited for long-term access and lateral movement across systems. In addition, real time revocation of such access can be difficult and create additional challenges when dealing with an incident. A more pragmatic approach focusing on efficient, periodic, user-initiated transfers or API access with reasonable duration limits seems more appropriate.

3) Frequency: requirements for granular dataset selection, date filters are positive steps aligned with stronger user control. However, overly prescriptive rules on reminder frequency (e.g., no more than quarterly for >12 month access) would undermine user awareness and control. It’s preferable to allow users to customize reminder preferences.

4) Safety and security vetting: while the DMA creates new data sharing obligations, it explicitly preserves GDPR protections (Recitals 6, 12, 59, and Article 8(1)). Designated companies must be permitted – and, where risks warrant, required – to conduct proportionate pre-transfer safety and security vetting of third-party data requesters and to provide appropriate risk disclosures without these being mischaracterized as dark patterns (paras. 125-127), as this undermines essential customer protections against nefarious actors. Companies must be allowed to conduct proper safety and security vetting of third-party recipients to meet their GDPR obligations, but also to protect customers from potential harm, as many third-party data requesters lack basic data security protections and may provide inconsistent information about their data protection practices. Thus, when a designated company receives a data portability request under Article 6(9) DMA, it must apply GDPR standards, including due diligence on third-party recipients and ensuring valid end-user authorization.

5) Effective switching and multi-homing: The Guidelines explain that per Recital 59 DMA, Article 6(9) is not only an enabler of effective switching and multi-homing but also of "innovation" in the digital sector (para. 103). While innovation can flow as a natural consequence of effective customer switching and multi-homing, it should not be a separate objective of the portability obligation in itself. Effective compliance of designated companies with the portability obligation can’t be possibly gauged against the level of innovation in the EU. Any such interpretation risks enabling data commercialization activities that go beyond

the DMA's intended purpose. Many third-party data requesters appear to be data aggregators seeking to commercialize personal data rather than providing services that would enhance contestability. The Guidelines should thus not expand the dataset beyond what is necessary to enable switching/multi-homing to avoid converting it into a general data-sharing right unrelated to contestability.

6) Tracking third-party data disclosures: the Guidelines require designated companies to provide a dashboard (para. 113) listing all recipients who received personal data of 3P individuals other than the requesting user. This creates an operationally impossible requirement where companies would need to track, maintain, and make accessible indirect data disclosures, including data about third parties that may be incidentally included in portability requests. Such a system would be extremely difficult (if not impossible) to implement accurately while potentially creating new privacy risks by making third-party data more visible, enabling personal information to be ported without meaningful consent. For example, an ex-romantic partner could port private messaging conversations to data aggregators in high-risk jurisdictions. The Guidelines must recognize that data portability requests involving third-party personal data require stronger safeguards beyond simple notification.

7) Overly broad approach to on-device portability: While on-device data should be portable when necessary for effective service switching or multi-homing, the Guidelines suggest a broader scope (paras. 109-110). This raises significant security concerns, as designated companies may not have access to or make use of these on-device data in their normal operations. Designated companies should not be required to expand their technological capabilities or route on-device data through their servers solely to enable such access, as this creates unnecessary security risks and complexity. The Guidelines should not create broader rights for designated companies to retain such data, and the scope should be strictly limited to the specific portability transaction.

8) Information about data portability risks: The Guidelines require portability options to be presented in a neutral and objective manner without nudging, without providing guidance on what constitutes improper nudging versus legitimate risk disclosure. As a result, even factual security warnings (such as information about third parties lacking basic privacy protections) could be mischaracterized as attempts to undermine portability. The Guidelines should recognize that such risk disclosures are not “nudging’ but are essential for enabling informed user choice and meeting GDPR transparency obligations.

The final Guidelines should provide clearer definitions for "generated data," reconsider the mandate for on-device data portability due to technical and security risks, and address the inherent conflicts in porting data concerning other individuals. The interpretation of "continuous and real-time" access should be pragmatic, focusing on effective API access rather than potentially unworkable indefinite synchronization. User control over reminders should be prioritized.

Article 6(10)

1) The Guidelines misinterpret Article 6(10)'s scope by shifting focus from business user data to general end user data. Article 6(10) of the DMA, supported by Recital 60, clearly focuses on two categories of data: (i) data provided or generated by business users, and (ii) data provided or generated by end users engaging with those business users' products or services. However, the Guidelines (paras. 147-148) expand this to include platform-observed data, general technical data like IP addresses, and broader end user platform behavior unrelated to end users' interaction with business users' products or services. This interpretation contradicts the DMA's text and imposes obligations beyond what the DMA intended, while distracting from the provision's core purpose.

2) Article 6(10) should allow flexible, user-configured durations for data portability, including "until withdrawn" by the end user While the DMA requires "continuous and real-time" access to data, this should be interpreted as ensuring reliable access when needed, not forcing indefinite access that could create security risks. The Guidelines require business users to have portability for "meaningful" periods of time, including indefinitely (para. 169). Business users should have control over access durations (one-time, fixed periods, or until withdrawn) with clear renewal options, and companies should be allowed to implement reasonable time caps (e.g., one year) to protect against security threats like fraud and account takeover. This is particularly crucial given that many third-party data requesters lack basic data security protections, provide inconsistent information about their data protection practices, and may operate in jurisdictions without adequate data protection standards. Without proper duration controls, continuous access could enable malicious actors to aggregate and exploit personal data over extended periods.

3) Granting business users access to data generated through their activities on a platform can support competition and innovation. However, the Guidelines' focus on end-user personal data (requiring consent) and the inclusion of on-device data introduce complexities regarding scope and technical feasibility:

    a. On-device Data: The inclusion of on-device data again raises significant technical implementation challenges and questions about access feasibility if the gatekeeper doesn't ordinarily process it as the Guidelines argue it should not result in gatekeepers having access to more on-device data.
    b. Consent Mechanism: Requiring gatekeepers to facilitate a consent interface between business users and end users for accessing personal data adds operational complexity. While gatekeepers should not be responsible for the validity of consent obtained by the business user (acting as controller), the practical implementation of such interfaces needs careful design to be user-friendly and avoid confusion.
    c. We recommend establishing that on-device data is out of the scope of the DMA. Additionally, the practical implementation of any mandated consent interface must be carefully specified to minimize operational complexity and avoid end-user confusion.

Article 6(11)

Providing access to anonymised search data requires an extremely high standard of anonymisation to protect user privacy effectively. All data access and interoperability obligations under the DMA must have robust, state-of-the-art privacy and security protections as a non-negotiable prerequisite. Technical anonymisation measures must be paramount, with contractual restrictions serving only as a secondary layer of protection:

1) Primacy of the GDPR: Privacy is a fundamental right, and the GDPR sets an "extremely high bar" for data protection requiring that the "likelihood of identification should be insignificant". The DMA does not override this. Specifically, the GDPR's standard for anonymization—a core requirement of Art. 6(11) —requires an "irreversible" process. Simple filtering techniques are "insufficient" as achieving this requires sophisticated technical measures.

2) Balancing Utility and Privacy: The mandate to adopt an anonymisation method that "preserves the most quality and usefulness" while also ensuring effective anonymisation highlights an inherent tension. Where a direct trade-off exists, the fundamental right to data protection must prevail. Methodologies should be chosen based on their proven effectiveness in preventing re-identification, even if this limits certain analytical possibilities for the data recipient

3) Consumer Trust and the "Security Liability Gap": Consumer trust is built on the secure handling of their data. The DMA's data-sharing mandates create a critical "security liability gap". Gatekeepers are legally obligated to share data, but the DMA imposes no new, specific security or compliance obligations on the data recipients. This creates a tangible "trading down' security risk" , where data moves from a highly secure environment to a potentially vulnerable one, with unclear liability in the event of a breach.

We demand the EDPB's Guidelines ensures privacy protections are not compromised. The Guidelines must explicitly state that any implementation of Art. 6(11) is conditional on robust, state-of-the-art security and full, demonstrable compliance with the GDPR's high anonymization standard. When balancing against data utility, privacy must be a non-negotiable prerequisite, not an afterthought.