Ein vereinfachter Rahmen für den Digitalsektor stärkt die gesamte EU-Wirtschaft

Ein leistungsfähiger und robuster digitaler Sektor ist entscheidend für wirtschaftliches Wachstum in Deutschland und die Wettbewerbsfähigkeit Europas. Dies erfordert eine langfristige Strategie für ein innovationsförderndes Unternehmensumfeld.

In den vergangenen Jahren hat die rasche, eng getaktete Einführung von fast 100 neuen technologieorientierten EU-Gesetzeswerken die Bewertung von Auswirkungen und Wechselwirkungen erschwert. Es ist entscheidend, die Folgen einer hohen Regulierungslast zu erkennen und sicherzustellen, dass sie unternehmerische Pläne, digitale Investitionen und die allgemeine Wettbewerbsfähigkeit der EU nicht behindern.

Daher begrüßen wir, dass die EU mit dem geplanten Omnibus zur Digitalgesetzgebung die Regulierungsdichte verringern will. Wichtig dabei ist, die bisher verabschiedeten EU-Gesetze zu vereinfachen sowie Überlappungen und Unklarheiten zu beseitigen. Neue Regulierung sollte vorher nicht auf den Weg gebracht werden.

Einige Anregungen im Detail:

Künstliche Intelligenz

KI hat das Potenzial, die Wettbewerbsfähigkeit Europas entscheidend voranzutreiben. Als grundlegende Technologie wird sie nicht nur neue, sondern auch etablierte Geschäftsmodelle beflügeln und Produktion, Forschung & Entwicklung sowie die Effizienz der öffentlichen Verwaltung unterstützen. Die Akzeptanz und Wirksamkeit dieser Technologie hängt jedoch davon ab, dass Unternehmen und Nutzer einen klaren und zuverlässigen Rechtsrahmen haben, um in KI zu investieren und ihre Mitarbeiter zu schulen. Deshalb haben wir uns entschieden, den **Code of Practice für Allzweck-KI** (GPAI - General Purpose AI) zu unterzeichnen.

Wir betrachten den Verhaltenskodex als einen Schritt hin zu einem berechenbaren regulatorischen KI-Umfeld, das die Einhaltung von Vorschriften vereinfacht und es Unternehmen ermöglicht, sich auf Entwicklung und Innovation zu konzentrieren. Die erheblichen Verbesserungen, die bereits vorgenommen wurden, wissen wir sehr zu schätzen.

Folgende Bedenken bleiben bestehen:

- **Herausfordernder und unsicherer Zeitplan**: Die Umsetzungsfristen für die GPAI-Modellbestimmungen bleiben für uns ein Anliegen. Während wir die Bemühungen anerkennen, die unrealistischen Zeitpläne anzupassen, hoffen wir auf ein stärkeres Entgegenkommen: Unternehmen müssen das komplexe Regelwerk in realistischer Zeit umsetzen können.

- **Urheberrecht**: Bestimmte Regelungen – insbesondere im Hinblick auf künftige Opt-out-Vorgaben und eine mögliche extraterritoriale Anwendung – bedürfen einer Auslegung mit Augenmaß, um nicht den Zugang zu KI zu gefährden.
- **Geschäftsgeheimnisse**: Es muss sichergestellt werden, dass Transparenzanforderungen nicht Geschäftsgeheimnisse offenlegen, die für den Wettbewerb und die Integrität der Modelle entscheidend sind.
- **Verhältnismäßigkeit**: Damit der AI Act Vertrauen und Innovation fördert, muss er zu einem stärker risikobasierten, verhältnismäßigen und zukunftssicheren Rahmen weiterentwickelt werden.

Cybersicherheit

Eine Vielzahl von EU-Gesetzen (z. B. NIS2, CRA, DORA, Cyber Solidarity Act, Cybersecurity Act, DSGVO) schaffen eine komplexe Lage für Cybersicherheits-Governance. Bestehende, international anerkannte Sicherheitsrahmen sollten genutzt werden, statt neue EU-spezifische Regularien zu schaffen. Nationale Zertifizierungssysteme, die von geltenden EU-Ansätzen oder internationalen Standards abweichen, sorgen nur für höhere Komplexität und Kosten, aber nicht für mehr Sicherheit.

- Bestehende Gesetze führen zu mehrfachen, sich überschneidenden Meldepflichten (DSGVO, DORA, NIS2, Cyber Resilience Act, AI Act).
    - Empfehlung: Vereinheitlichung mit einem einzigen Portal und Prozess zur Meldung von Vorfällen an eine zentrale Stelle. Harmonisierung der Schwellenwerte und Fristen nach dem Vorbild von NIS2.
- **Eine Angleichung von Pflichten in den Bereichen Desinformation, Cybersicherheit, Nachhaltigkeit und Datenverarbeitung ist geboten.** Beispiel: Im Rahmen der Regulierung digitaler Inhalte auf EU-Ebene müssen derzeit acht verschiedene, sich überschneidende Berichtspflichten erfüllt werden. Diese Berichte sollten zusammengeführt oder zumindest mit einheitlicher Taxonomie, Zeitrahmen und Metriken versehen werden (siehe Tabelle im Anhang)**.**

Wettbewerbs- und Kartellrecht

DMA: Das Verbot der Selbstbevorzugung im Digital Markets Act [Art. 6 (5)] muss präzisiert werden, um unnötige wirtschaftliche Schäden zu vermeiden und Innovation zu ermöglichen.

- Eine neue Studie der Copenhagen Business School zeigt: Der DMA verursacht erhebliche wirtschaftliche Belastungen in der EU-Wirtschaft – bis zu 114 Milliarden € an Umsatzeinbußen, insbesondere in Branchen, die stark auf digitale Plattformdienste angewiesen sind.
- Die Studie schätzt jährliche Umsatzverluste pro Arbeitnehmer auf bis zu 1.122 €, abhängig vom Digitalisierungsgrad der jeweiligen Branche. EU-Verbraucher müssen rund 50 Prozent mehr Suchanfragen stellen, um Hotels, Restaurants oder Produkte zu finden.

- Buchungs-Traffic für Hotels und Fluggesellschaften aus der EU ist signifikant gesunken (geschätzte bis zu 14 Milliarden € jährlicher Schaden für Hotels).
- Im Rahmen von Tests zur DMA-Umsetzung haben wir im Dezember 2024 weitere Hotelfunktionen aus der Google-Suche entfernt – diese zeigten: Hotels würden neuerlich mehr als zehn Prozent an Traffic verlieren, was europäische Hotels zusätzlich schädigen würde.
- Auch der Einzelhandel in der EU ist betroffen (geschätzter Schaden bis zu 59 Milliarden € jährlich).

Auch bereits bestehende Gesetze, Verordnungen und Vorgaben mit Fokus auf die Digitalwirtschaft, die in der Vergangenheit zusätzlich zu geltendem EU-Recht in einzelnen Mitgliedsstaaten beschlossen wurden, müssen überprüft werden. Wenn sich zeigt, dass nationale Regulierung unnötige Komplexität schafft, muss sie kritisch hinterfragt werden. Dies gilt insbesondere für das deutsche Regelwerk des § 19a GWB, das parallel zum europäischen DMA existiert. Beide Regelwerke **überschneiden sich inhaltlich stark**. Der DMA schafft in der Theorie eine Struktur mit unmittelbaren und langfristigen Vorteilen: Vermeidung doppelter Verfahren, Verkürzung von Bearbeitungszeiten durch Wegfall von Zuständigkeitsstreitigkeiten, Konzentration nationaler Behörden auf ergänzende Durchsetzungsmaßnahmen.

- Doch neben diese eigentlich EU-weit abschließende Systematik des DMA für seine 27 Mitgliedsstaaten setzt nur in Deutschland §19a GWB das Konzept von “Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb” im Digitalbereich. Unter dieser Norm wurden bisher fünf US-amerikanische Unternehmen designiert – kein einziges europäisches oder anderes internationales Unternehmen. Das Bundeskartellamt kann Maßnahmen in Märkten ergreifen, **in denen die betroffenen Unternehmen keine dominante Stellung haben** – um **hypothetische zukünftige Wettbewerbsschäden** zu verhindern.

Verbraucherrechte und Inhalteregulierung (mehr dazu in den Detailed Recommendations im Anhang)

Deutschland sollte sich für den **Abbau überlappender Pflichten** einsetzen, um Rechtssicherheit und unternehmerische Handlungsfreiheit in der EU zu verbessern. Insbesondere sollten Transparenzberichte und Risikobewertungen vereinfacht und AVMS-Richtlinienbestimmungen gestrichen werden, die durch den DSA bereits ersetzt wurden (z. B. zur Inhaltemoderation und zum Jugendschutz).

Der Draghi-Report hat verdeutlicht, dass fragmentierte Vorschriften, insbesondere in Bereichen wie dem Datenschutz, Hindernisse für Innovation und Wachstum schaffen. Europa hat bereits die strengsten Verbraucher- und Datenschutzstandards weltweit. Eine weitere Regulierung könnte Innovationen ersticken und großen wie kleinen Unternehmen schaden. Politische Entscheidungsträger sollten die Notwendigkeit neuer Gesetze kritisch prüfen und stattdessen auf die Durchsetzung der zahlreichen Vorschriften setzen, die bereits für die im **Digital Fairness Act** genannten Bereiche gelten:

- Die DSGVO regelt bereits die Verarbeitung personenbezogener Daten.
- Der DSA hat weitere Beschränkungen für das Targeting von Minderjährigen und das Targeting auf der Grundlage sensibler Daten eingeführt.
- Der DMA führte neue Regeln für den produktübergreifenden Datenaustausch ein.
- Die Verbraucherrechterichtlinie regelt die Offenlegung personalisierter Preise.
- Die im „Digital Fitness Check“ des EU-Verbraucherrechts identifizierten Mängel deuten nicht auf fehlende Regeln hin, sondern auf eine mangelhafte Durchsetzung und den Bedarf an praktikabler Umsetzbarkeit.

Daten und Datenschutz (mehr dazu in den Detailed Recommendations im Anhang)

Die angestrebte Vereinfachung des Datenschutzes in Deutschland aus dem Koalitionsvertrag ist wichtiger denn je. „Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an. Sie soll dann Bundesbeauftragte für Datennutzung, Datenschutz und Informationsfreiheit sein.“ (S. 65). Deshalb ist ein mehr **risikobasierter Ansatz für die DSGVO** geboten. Das bedeutet, dass Vorschriften verhältnismäßig und nicht absolut angewendet werden sollten, um die Belastung für Unternehmen je nach Risikoniveau einzustufen.

- Die Legitimation **berechtigter Interessen** sollte als rechtliche Grundlage weiterhin ausreichen – wie es der EDSA in seiner Stellungnahme vom Dezember getan hat. Einwilligung darf nicht die einzige Option für wirksamen Datenschutz sein.
- Die Einführung einer Positivliste von Verarbeitungsvorgängen, bei denen berechtigtes Interesse angemessen ist, würde mehr Klarheit schaffen. Dies sollte auch Fälle umfassen, in denen etablierte, überprüfbare datenschutzfördernde Technologien (PETs) eingesetzt werden.
- **Eine Präzisierung der DSGVO-Regeln zu besonderen Kategorien personenbezogener Daten (SCD)**, würde helfen, verantwortungsvolle KI-Innovation zu unterstützen**:**
    - Die aktuell weit gefassten Auslegungen und wenigen Ausnahmen schaffen rechtliche Unsicherheit bei der Nutzung von SCD für wissenschaftliche Forschung, zur Bekämpfung von Bias oder zur Verbesserung der kulturellen und regionalen Repräsentativität von KI-Modellen.
    - Klare Regeln für die Verarbeitung von Daten, die von Einzelpersonen offensichtlich publik gemacht wurden (mit geeigneten Schutzmaßnahmen).
    - Die Entwicklung von General-Purpose-KI-Modellen für wissenschaftliche Forschung sollte ausdrücklich als Ausnahme anerkannt werden.

Anhang: Auszug ausgewählter Berichtspflichten

Bericht	Location	Turnus
EU DSA (VLOP/VLOSE report)	Transparenzbericht Website	Bi-annual
EU DSA (non VLOP report)	Transparenzbericht Website	Jährlich
Information about Monthly Active Recipients under the DSA (EU DSA MAR)	Transparenzbericht Website	Halbjährlich
Strengthened EU Code of Practice on Disinformation (EU CoP)	Direkt an Regulierungsbehörde; Veröffentlichung im EC Transparency Center	Halbjährlich
EU Terrorist Content Online (EU TCO)	Transparenzbericht Website	Jährlich

Suggested change	Justification
SIMPLIFICATION #1 - RECOMMENDER SYSTEMS	
1. Abstain from further regulating this space. We are concerned by rumors that the Digital Fairness Act may include even more regulatory requirements for recommender systems used by online platforms. 2. Withdraw the recommender system requirement under the Platform to Business Regulation.	1. The EU institutions should be working to simplify the regulatory framework applicable to recommender systems used by online platforms instead of further adding to it. 2. The recommender system requirement under the Platform to Business Regulation is no longer required. The Platform to Business Regulation regulates recommender systems for business users. Article 27 of the Digital Services Act now regulates recommender systems for both end and business users under a more centralised enforcement model.
SIMPLIFICATION #2 - DARK PATTERNS	
1. Abstain from further regulating this space. We are concerned by rumors that the Digital Fairness Act may add to the already fragmented regulatory landscape for dark patterns. 2. Consider withdrawing Article 25 of the Digital Services Act.	1. The EU institutions should be working to simplify the regulatory framework applicable to dark patterns online instead of further adding to it. 2. According to Article 25(2) of the Digital Services Act, the dark patterns regulation in the Digital Services Act shall not apply to practices covered by the Unfair Commercial Practices Directive and the General Data Protection Regulation. It is unclear what additional policy imperative Article 25 of the Digital Services Act intends to cover.
SIMPLIFICATION #3 - TRANSPARENCY REPORTING	
1. Ensure there is no duplication of metric requirements across different transparency reports (including as regards any future regulations). Extend deadlines to produce transparency reports to at least 2 months after the end of the reporting	1. This would streamline reporting and avoid duplication of efforts. It would also make review by third party stakeholders easier.

period. 2. Change the requirement for the Disinformation Code of Practice reporting to an annual cadence rather than a biannual one. 3. Withdraw the transparency reporting requirements under the Platform to Business Regulation.	2. The Disinformation Code of Practice transparency report is extremely burdensome to produce, given the inclusion of granular data points and extensive narratives. For many commitments there are no updates within the last 6 months, making production of the report bi-annually disproportionate. 3. The transparency reporting requirement of the Platform to Business Regulation is no longer required, as the transparency reporting under the Digital Services Act includes information about complaints relating to content moderation actions by both end- and business- users.
SIMPLIFICATION #4 - MINORS' PROTECTION ONLINE	
1. Withdraw Article 28b of the Audiovisual Media Services Directive, to avoid the proliferation of fragmented and contradictory Member State laws implementing that provision. Focus on implementing Article 28 of the Digital Services Act.	1. The Digital Services Act fully harmonises minors' protection online, superseding any Member State implementation of the pre-existing Audiovisual Media Services Directive requirement.
SIMPLIFICATION #5 - CONTENT MODERATION REQUIREMENTS	
1. Withdraw Article 28b of the Audiovisual Media Services Directive, to avoid overlaps with the Digital Services Act and the proliferation of fragmented and contradictory Member State laws implementing that provision. Focus on enforcing the overlapping requirements in the Digital Services Act.	1. The Digital Services Act fully harmonises content moderation requirements applicable to intermediary services (including video-sharing platforms), rendering obsolete such requirements in the Audiovisual Media Services Directive, and superseding their implementation by Member States.
SIMPLIFICATION #6 - RISK ASSESSMENTS	
1. Abstain from further regulating this space. We are concerned to see proposals that a distinct risk assessment requirement be imposed on intermediary services already regulated under the Digital Services Act as regards the presence of CSAM specifically on their services. 2. Issue non-binding guidance on the overlaps across EU laws as	1. Risk assessments produced by very large online platforms and very large online search engines under the Digital Services Act already account for risks related to CSAM. There is no need for a separate, additional risk assessment. 2. This will help companies understand (a) how to craft their risk assessments in a manner that fulfills multiple regulatory

regards risk assessments.	requirements, and (b) when they are exempt from providing additional risk assessments.
SIMPLIFICATION #7 - DSA VLOP/SE DESIGNATION	
1. Continue relying on monthly active recipient counts to determine whether VLOP/SE designation may be considered; but introduce additionally the possibility for a dialogue between the European Commission and the relevant provider to exempt the service at issue from designation on the basis of its risk profile.	1. The current VLOP/SE designation process does not take into account the risk profile of services, and subjects a wide range of providers to the most burdensome Digital Services Act requirements solely on the basis that those are popular with users.
SIMPLIFICATION #8 - INTERNAL GOVERNANCE	
1. Providers of digital services should be left with a high level of discretion on how to manage compliance oversight internally. 2. Requirements regarding "independence", "authority" and "composition" of internal compliance structures should be harmonised.	1. Every organisation is different and should be granted flexibility to put in place the information flows and processes that best cater to its specific structure and mode of operation. 2. Different requirements imposed on internal compliance structures create organisational complexity.
SIMPLIFICATION #9 - TRADE SECRETS PROTECTION	
1. Ensure consistent and robust protection of trade secrets through the interpretation of the relevant EU Data Act, EU Copyright Directive, and AI Act requirements. 2. Issue follow-up instruments (e.g. in the framework of the AI Act Code of Practice/Model Documentation Form) to clarify how it will be ensured that trade secrets are protected. Among other elements, and consistent with Recital 14 of the Trade Secret Directive, it should be reflected in these instruments that the commercial value criterion is generally understood and applied by Courts as referring to the actual or potential commercial value of the information, due to its secrecy and the competitive advantage it confers on its holder.	1. To maintain innovation incentives, there needs to be clear guidance and signals provided by regulators that data sharing and transparency requirements may not be used as backdoors to getting access to trade secrets of other companies. 2. Trade secrets are protected by several international (Article 39 TRIPS), regional and national legislations (the Trade Secret Directive has been implemented in all member states)

GDPR

Index

SIMPLIFICATION #1 - Explicitly recognise the proportionality principle in the GDPR	
Suggested change	Justification
Potential Change 1 - Targeted amendment to Article 24(1) to recognise proportionality of measures applied to demonstrate compliance with GDPR *1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate and proportionate technical and organisational measures to ensure and to be able to demonstrate*	- **Potential Changes 1 and 2** seek to more explicitly recognise the proportionality principle in Article 24 GDPR. The rationale is that the recognition of this principle will afford controllers additional flexibility in interpreting the GDPR's obligations in a manner that is proportionate to risk/cost thereby reducing the compliance burden currently placed on them. - In addition, this would create additional legal certainty for organisations in complying with the GDPR's obligations

that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. **<u>Potential Change 2 - Addition of a new Article 24(4) GDPR recognising proportionality principle more generally</u>** *4. The obligations imposed on the controller by this Regulation shall be interpreted in accordance with the principle of proportionality, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the controller's reasonable assessment of the risk of varying likelihood and severity for the rights and freedoms of natural persons.*	because they would be afforded some latitude by DPAs interpreting the GDPR's in a manner that is proportionate to e.g. the risk arising from the processing. - This would also recognise that controllers may be best placed to assess the actual risks to data subjects and assess which compliance measures are proportionate.

SIMPLIFICATION #2 - Simplify and afford controllers flexibility in complying with the GDPR's accountability principle, in particular where Article 6(1)(f) GDPR is relied on as a lawful basis.	
Suggested change	Justification
<u>Potential Change 1 - Amend Article 6(1)(f) GDPR to recognise a 'whitelist' of processing activities which are presumptively lawful.</u> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. The Commission shall in accordance with the examination procedure referred to in Article 93(2) adopt an implementing act containing a list of the kind of processing operations which are presumed to be*	- **Potential Change 1** seeks to introduce in Article 6 GDPR a 'whitelist' of legitimate interests for which the balancing exercise for reliance on legitimate interests is presumed to favour a controller. This list could include specific types of lower-risk processing activities like fraud/abuse protection; product improvement; debugging/ product maintenance (i.e. in effect the opposite of the Article 35 lists of high risk processing adopted by DPAs). In addition, this amendment seeks to afford controllers a 'margin of appreciation' in applying the legitimate interests assessment test for these processing activities. The rationale is to introduce some degree of legal certainty to reliance on legitimate interests

lawful based on point (f) of Article 6 of this Regulation. The controller shall be afforded a margin of appreciation in its assessment of whether these processing operations are necessary for the purposes of the legitimate interests pursued by a controller or by a third party, and whether such interests are overridden by the interests or fundamental freedoms of the data subject. **Potential Change 2 - Amend Article 5(2) to reduce duplicative measures** *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). A controller may rely on a single set of measures to demonstrate compliance for a set of processing operations that are similar in terms of their nature, scope, context and purpose.*	as a lawful basis (which is typically the basis relied on by organisations for purposes such as product improvement and research) and to afford controllers with some flexibility in carrying out these assessments where certain basic criteria are met. At present, organisations face significant uncertainty in whether their lawful basis will be upheld, even when they have carried out assessments in line with regulatory guidance, creating legal uncertainty and hampering innovation. This might also raise the possibility of codifying certain aspects of guidance on new technologies, e.g. giving legal effect to the position in the EDPB's AI Models Opinion that the training of AI models on publicly available personal data is lawful in principle. - **Potential Change 2** seeks to amend Article 5(2) to explicitly recognise that controllers can rely on the same accountability measures and documentation for a similar set of processing operations. This aims to introduce additional flexibility for controllers to rely on a single assessment for similar sets of processing activities, thereby reducing the compliance burden currently placed on organisations for example when conducting research and development related processing activities using personal data.

SIMPLIFICATION #3 - DSARs: Introduce a 'disproportionate efforts' exemption to compliance with Articles 15-22 GDPR	
Suggested change	Justification
Potential Change 1 - Amend Article 12(5) to introduce a	- **Potential Change 1** seeks to introduce a disproportionate

‘disproportionate efforts’ exemption to responding to a DSAR *5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge.* *Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, or, taking into account the scope of the processing and the cost of implementation, where responding to the request would involve a disproportionate effort, the controller may either:* *(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or* *(b) refuse to act on the request.* *The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of, or the disproportionate efforts involved in responding to, the request.* **Potential Change 2 - Allow controllers to provide standardised information to discharge their obligations to respond requests for information under Article 15 GDPR** *(1) The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. In cases where a controller provides services or products to data subjects on a standardised basis, in particular in connection with provision of online services, a*	efforts exemption in Article 12(5) to respond to data subject rights requests. While Google recognises that it is important to facilitate the exercise of rights of data subjects under the GDPR, the intention of this change is to allow for a limited exception allowing controllers to demonstrate that responding to rights requests involves disproportionate effort. Similar exemptions exist for other GDPR articles (Article 14). Introducing this change would give organisations scope to refuse to respond to requests where the cost and operational lift of doing so is wholly disproportionate. - **Potential Change 2** seeks to allow controllers, who provide standardised services to users, to respond to requests for information under Article 15 using standardized notices or information (e.g. by referring the data subject to a publicly available privacy policy). This avoids the need for controllers to provide bespoke information where this information is common to many data subjects. The current draft of the GDPR is ambiguous as to whether this is permissible; an interpretation that requires the provision of bespoke information would be wholly unworkable and unnecessarily burdensome for many controllers (because it would require extensive searches of systems, and the identification and verification of this information for every request), including SME’s. This amendment seeks to balance the provision of useful information to data subjects while reducing the burden placed on controllers.

controller may provide the information referred to Articles 13 and 14 and any communication under Articles 15 to 22 and 34 in a standardised form, including by making this information publicly available. ***New recital*** *(..) This Regulation recognises that many controllers provide services on a standardised basis, particularly for online services, where the core features and functionalities offered as part of those services are the same for all users, provided under common terms of service and involving broadly the same categories of personal data and processing purposes and operations. In such a case, particularly where users are provided with the requisite transparency information and choose to use services through the creation of an online account, it would be disproportionate to require a controller to give effect to the rights of information and access to personal data on an individualised basis where the same result can be achieved substantively as effectively using standardised information and/or tools made available to all users.*	

SIMPLIFICATION #4 - Narrow the scope of the personal data that constitutes special category data under Article 9 GDPR and/or introduce more flexible exemptions under Article 9(2) GDPR	
Suggested change	Justification
Potential change 1 - narrow the definition of SCD in Article 9(1) *(1) The following shall be prohibited:* *(a) the processing of personal data that explicitly and directly concerns ~~revealing~~ racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, ~~and the~~*	- **Potential Change 1** seeks to clarify the concept of SCD in Article 9 GDPR by limiting its scope to 'explicit' SCD (this concept has a basis in guidance issued by the EDPB) and non-explicit SCD where a controller is seeking to draw inferences based on sensitive categories. While Google recognises that it is important to afford additional protections to data that is sensitive, the concept of SCD as it

(b) the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, *(c)* the processing of *data concerning health or data that explicitly and directly concerns ~~concerning~~ a natural person's sex life or sexual orientation ~~shall be prohibited.~~* *(d) the processing of personal data for the purpose of profiling or drawing inferences about the data subject on the basis of the categories of information mentioned in points (a) and (c).* *Article 4* *15. 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which explicitly and directly reveals information about his or her health status;* **Potential Change 2 - Expand the SCD exemptions in Article 9(2)** *2. Paragraph 1 shall not apply if one of the following applies:* *[..]* *(e) processing relates to personal data that is publicly available and where the controller takes appropriate measures to protect the data subject's rights and freedoms and legitimate interests, in particular to ensure respect for the principle of data minimisation; ~~which are manifestly made public by the data subject;~~* *[...]* *(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or*	is currently interpreted is overbroad to the extent that it means potentially any data could constitute SCD if it permits inferences of a sensitive nature to be drawn. This legal uncertainty hampers innovation as organisations are left unsure as to whether they have a lawful basis to process this type of data. - **Potential Change 2** seeks to expand the exemptions in Article 9(2) to allow for flexibility for organisations to process SCD where appropriate safeguards are adopted. Expansion of the Article 9(2) exemptions would assist many organisations, including SMEs seeking to innovate in the AI space by training LLMs and other models in a manner that is consistent with the EU's AI Act. - **Potential Change 3** seeks to enshrine the CJEU's pragmatic approach to a controller's responsibility for Article 9 in *GC & Others*. Recognition of these principles more generally in the GDPR would allow for additional flexibility for organisations seeking to innovate in the AI space by recognising that a controller's responsibility for compliance with Article 9 should take into account the specific features of the processing.

Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The development of a general-purpose AI model in accordance with Article 89(1) and Chapter V of Regulation (EU) 2024/1689 shall constitute a scientific research purpose for the purposes of this Regulation; *(k) processing is necessary for compliance with a legal obligation to which the controller is subject.* **Potential Change 3 - Codify CJEU's ruling GC & Others in a new Article 9(5)** *5. Any assessment of the controller's compliance with this Article should be carried within the framework of the controller's responsibilities, powers and capabilities. The extent of a controller's responsibility for compliance should take account of the specific features of the processing at issue.*	

SIMPLIFICATION #5 - Streamline the GDPR's data transfer regime	
Suggested change	Justification
Potential Change 1 - Add a new paragraph 6 to Article 46 to provide for an intra-group data transfers certification mechanism *6. The Commission shall adopt an implementing act in accordance with the examination procedure referred to in Article 93(2) that specifies certain principles and categories of safeguards a controller may adopt for cross-border transfers to third countries of personal data between undertakings in the controller's corporate group in the*	- **Potential Change 1** seeks to enshrine in the GDPR a certification regime for intra-group transfers. Signing up to this self-certification regime would obviate the need to carry out TIAs/SCCs for transfers outside the EEA, which would significantly reduce the compliance burden faced by organisations. Further input would be needed on the specifics of such a regime. - **Potential Change 2** seeks to reduce the compliance burden that organisations who rely on SCCs face to transfer data

absence of a decision pursuant to Article 45(3). Those principles shall facilitate the global transfer between undertakings of personal data processed in the ordinary course of business and shall have regard to the varying corporate and legal structures of global businesses, as well the protection for data subjects that may be afforded by a group's compliance, including on a voluntary basis, with this Regulation outside the EEA as well as relevant technical and organisational measures implemented groupwide. *7. A controller that self-certifies adherence by its group with the principles referred to in Article 46(6) shall be presumed to have provided appropriate safeguards within the meaning of paragraph 1, for transfers between group undertakings without the obligation to conduct case-by-case assessments of the level of protection otherwise afforded to the relevant personal data in relevant third countries.* **Potential Change 2 - Amend Article 46 to introduce additional flexibility to the assessments of third country laws for the purposes of the SCCs** *(1) In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. To that end, the controller or processor transferring personal data to a third country shall carry out an assessment of the level of protection afforded in the context of such a transfer, taking into account:* *(a) the appropriate safeguards used by the controller or processor for the transfer; and* *(b) as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the*	outside the EEA by recognising that organisations may rely on the same assessment for a similar set of transfers, where the same set of safeguards are used. The intention of this change is to allow organisations to conduct a 'global TIA', where appropriate, reducing the significant burden placed on organisations in potentially conducting multiple, often duplicative, assessments for every transfer they carry out. - **Potential change 3** contains a simple change to the current SCC decisions to address the current gap/legal uncertainty faced by many organisations who transfer data outside the EEA to organisations that are subject to GDPR. This would avoid the need for the Commission to adopt an entirely new decision.

legal system of that third country, in particular, those set out, in a non-exhaustive manner, in Article 45(2) of this Regulation, and the practical likelihood of public authorities seeking or being granted access to the personal data transferred. *A single assessment may address a set of similar transfers, including where the same or a similar set of appropriate safeguards are used.* **Potential Change 3 - Update Article 1 of the SCC Commission Decision so that the SCCs apply to transfers to organisations established in third countries that are subject to GDPR.** ***Article 1*** *The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor established in a third country ~~whose processing of the data is not subject to that Regulation (data importer).~~*	

SIMPLIFICATION #6 - Clarify the circumstances in which parties are deemed to be 'joint controllers'	
Suggested change	Justification
Potential Change 1 - Define the concept of joint controllership in Article 4 and amend Article 26 *(27) 'joint controller' means two or more controllers that expressly agree by way of an arrangement to jointly determine the purposes and means of processing.*	- **Potential Changes 1 and 2** seeks to clarify the definition of joint controllership so that, to be in a joint controllership, the parties must expressly agree to be joint controllers, whether by contract or similar express legal arrangement. This aims to address the significant legal uncertainty that exists at present where organisations may be unintentionally responsible for processing, contrary to their intentions and

Article 26 *Joint Controllers* *1. ~~Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They~~ Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of the ~~an~~ arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.* ***(Alternative to the above) Potential Change 2 - Amend Article 26(1)*** *Where two or more controllers expressly agree by way of an arrangement to jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of the ~~an~~ arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.* ***Potential Change 3 - Amend Article 82 to restrict liability of joint controllers*** *2. ~~Any~~ A controller ~~involved in processing~~ shall be liable for the damage caused by processing it controls which infringes this Regulation. A processor shall be liable for the damage caused by*	terms agreed with counterparties. - **Potential Change 3** seeks to limit the liability for controllers to processing that it controls (rather for processing that it is "involved in"). The intention is to limit situations where an independent controller is found to be liable for processing which it does not solely control. In addition, the suggested change to Article 83(2) seeks to limit the situations in which parties may be held jointly and severally responsible for situations where the parties are in a joint controllership relationship (which, per the suggested changes to Article 26/4, the parties must expressly agree to enter into). The overall rationale for these changes is to create additional legal certainty for organisations as to their liability under the GDPR when they engage in processing activities/contract with other parties.

processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. *3. A controller or processor shall be exempt from liability under paragraph 2 if it ~~proves that it~~ is not in any way responsible for the event giving rise to the damage.* *4. ~~Where more than one controller or processor,~~ Joint controllers, or both a controller and a processor, that are involved in the same processing and that ~~where they~~ are, under paragraphs 2 and 3, responsible for any damage caused by processing, ~~each controller or processor~~ shall each be held liable for the entire damage in order to ensure effective compensation of the data subject.*	

ePrivacy Directive

SIMPLIFICATION #1 - Extend the exception to the Article 5(3) ePD consent requirement for cookies and other on-device data access/storage for security purposes	
Suggested change	Justification
Amend A5(3) ePD to expand the scope of the exemptions to security cookies *3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC inter alia, about the purposes of the processing. This shall not prevent any technical storage or access:*	• This potential change seeks to bring up to date the Article 5(3) rules on on-device processing to reflect the reality of how organisations process data in today's online environment. While Google appreciates Article 5(3)'s rationale for protecting the untoward access to or storage of information on a user's device as part of the user's "private sphere", the current rules are overly restrictive and create unnecessary barriers to many valid and low-privacy impact uses of cookies and similar technologies. • Moreover, the regulatory status quo means that storage/access

(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network~~, or~~ ; *(b) as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service;* *(c) necessary to ensure or restore the security of, or detect technical faults or errors in, electronic communications networks and services (and related services and devices).* *(d) necessary to detect or prevent the fraudulent use, abuse or manipulation of electronics communications networks and services (and related services and devices) by a user, subscriber or other party, including where such conduct affects the rights and legitimate interests of others or undermines the integrity of the network or service.;*	to data on-device is subject to more stringent rules than, e.g., cloud-based processing, where technological developments mean products/features now keep data on-device by design, and precisely because it can be more privacy-protective. • The suggested additions of points (c) and (d) to Article 5(3), seeks to permit access to/storage of information on a user's device (e.g. the use of cookies) where this is necessary for valid use-cases such security/product maintenance and fraud and abuse detection, including where abuse/manipulation of a service impacts the rights/interests of other stakeholders (e.g. customers who rely on the service). This change will benefit users and industry in that it seeks to ensure that online services are provided securely using on-device processing methods. • Overall, the changes aim to enhance legal certainty for organisations operating in the online environment (including SME's), many of whom rely on cookie/similar technology to ensure the security of their services. • From a user perspective, more flexible rules on user consent would likely mean a reduction in the display of cookie-banners and the related "click fatigue" that users currently face online. Clarifying these rules would also address the legal uncertainty and friction in the internal market caused by the inconsistent interpretation by regulators of the current rules.

SIMPLIFICATION #2 - Extend the exception to the Article 5(3) ePD consent requirement for cookies and other on-device data access/storage for analytics purposes	
Suggested change	Justification

Amend A5(3) ePD to expand the scope of the exemptions to analytics cookies *3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC inter alia, about the purposes of the processing. This shall not prevent any technical storage or access:* *(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network~~, or~~ ;* *(b) as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service;* *(c) necessary for web audience measurement.* *New Recital - web audience measurement:* *The concept of web audience measurement referred to in Article 5(3)(e) of this Directive includes the measurement of traffic to a website, app or service with a view to understanding how the website, app or service is used, provided that this measurement does not entail the profiling of users across websites, apps or services.*	• This potential change seeks to bring up to date the Article 5(3) rules on on-device processing to reflect the reality of how organisations process data in today's online environment. While Google appreciates Article 5(3)'s rationale for protecting the untoward access to or storage of information on a user's device as part of the user's "private sphere", the current rules are overly restrictive and create unnecessary barriers to many valid and low-privacy impact uses of cookies and similar technologies. • Moreover, the regulatory status quo means that storage/access to data on-device is subject to more stringent rules than, e.g., cloud-based processing, where technological developments mean products/features now keep data on-device by design, and precisely because it can be more privacy-protective. The suggested additions of point (c) to Article 5(3) and the corresponding recital seek to permit on-device access/storage for analytics-related use-cases. Clearer and more flexible rules on when on-device access/storage is permissible for analytics purposes will reduce the barriers to innovation and legal uncertainty caused by the current rules. • Overall, the changes aim to enhance legal certainty for organisations operating in the online environment (including SME's), many of whom rely on online advertising and other cookie/similar technology related uses for revenue, or to ensure the security/improve their services. • From a user perspective, more flexible rules on user consent would likely mean a reduction in the display of cookie-banners and the related "click fatigue" that users currently face online. Clarifying these rules would also address the legal uncertainty and friction in the internal market caused by the inconsistent interpretation by regulators of the current rules.

SIMPLIFICATION #3 - Extend the exception to the Article 5(3) ePD consent requirement for cookies and other on-device data access/storage to permit the display of contextual advertising to users	
Suggested change	Justification
<u>Amend A5(3) ePD to expand the scope of the exemptions to permit the display of contextual advertising to users</u> *3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC inter alia, about the purposes of the processing. This shall not prevent any technical storage or access:* *(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network~~, or~~ ;* *(b) as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service;* *(c) necessary for the display of contextual advertising to the user.* *New Recital - contextual advertising* *The concept of contextual advertising referred to in Article 5(3)(f) means online advertising that is selected using data collected from a single session during which a user interacts with a website, app or service, which may include the selection of advertising based on (i) the content the user is currently interacting with, (ii) in the case of a search engine, their current query, and/or (iii) the user's current device.*	• This potential change seeks to bring up to date the Article 5(3) rules on on-device processing to reflect the reality of how organisations process data in today's online environment. While Google appreciates Article 5(3)'s rationale for protecting the untoward access to or storage of information on a user's device as part of the user's "private sphere", the current rules are overly restrictive and create unnecessary barriers to many valid and low-privacy impact uses of cookies and similar technologies. • Moreover, the regulatory status quo means that storage/access to data on-device is subject to more stringent rules than, e.g., cloud-based processing, where technological developments mean products/features now keep data on-device by design, and precisely because it can be more privacy-protective. • The suggested additions of point (c) to Article 5(3) and the corresponding new recital seek to permit on-device access/storage to display contextual advertising to users. Clearer and more flexible rules on when on-device access/storage is permissible for contextual advertising purposes will reduce the barriers to innovation and legal uncertainty caused by the current rules. • Overall, the changes aim to enhance legal certainty for organisations operating in the online environment (including SME's), many of whom rely on online advertising and other

	cookie/similar technology related uses for revenue. • From a user perspective, more flexible rules on user consent would likely mean a reduction in the display of cookie-banners and the related "click fatigue" that users currently face online. Clarifying these rules would also address the legal uncertainty and friction in the internal market caused by the inconsistent interpretation by regulators of the current rules.

SIMPLIFICATION #4- Clarify that displaying a cookie banner is not required where one of the Article 5(3) exemptions is relied on (i.e. when user consent is not required)	
Suggested change	Justification
Add a new Article 5(4) ePD that clarifies that a cookie-banner is not required to be surfaced to a user where eDP consent is not sought *4.* Entities carrying out activities covered by Article 5(3) shall be afforded discretion as to the manner in which the clear and comprehensive information referred to in that Article is provided. *New Recital [x]* *The provision of clear and comprehensive information referred to in Article 5(3) of this Directive shall not require, in relation to activities covered by points [(a) - (e) of Article 5(3)], the use of so-called "cookie banners", provided that the requisite information is displayed in a notice that is easily accessible to the user. The information provided for the*	• Similar to the Simplifications above, this change seeks to clarify the rules on on-device access to/storage of information (in particular the use of cookies) and enhance certainty for organisations operating in the online environment. Many organisations (including SME's) rely on cookies/similar technologies to ensure the security of or improve their services (e.g. using analytics). This clarification would address the significant legal uncertainty and friction in the internal market caused by the inconsistent interpretation by regulators of the current rules. • From a user perspective, more flexible rules on user consent would likely mean a reduction in the surfacing of cookie-banners and the related "click fatigue" that users currently face online. Where consent is not required, there is

purposes of Article 5(3) should be comprehensive as to the purposes of the processing. The provision of comprehensive information in relation to the cookies or other similar technologies used to store or access information on the user's terminal equipment shall not be required.	little privacy benefit to overburdening a user with this information, when they can easily access it in a privacy policy or notice if they so wish.

SIMPLIFICATION #5- Clarify that "the storing of information, or the gaining of access to information already stored" is not intended to capture ephemeral storage and/or information transmitted as part of ordinary internet connectivity	
Suggested change	Justification
<u>Amend A5(3) ePD to clarify what is meant (or rather, not meant) by "storage" and "access"</u> *3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. Storage and gaining access in this paragraph 3 shall not include mere transient or ephemeral storage, or operations which form part of the ordinary exchange of information from the terminal equipment when a user or subscriber accesses an information society service.*	• Google welcomes the EDPB's work to clarify Article 5(3) and so provide greater certainty to online operators. However, we propose this update, which affirms the role of the GDPR as the overall framework for regulating the processing of personal data, with ePrivacy operating as a more targeted *lex specialis* regime. • The intent of the amendment is to ensure that information which is communicated as part of the ordinary operation of the internet (e.g. as part of the Transmission Control Protocol / Internet Protocol) or the device, and is not targeted by the sender/recipient, is outside of the scope of Art 5(3). • An overly broad interpretation of Art 5(3) which inadvertently captures data transmitted as part of the ordinary workings of the internet does not further the overall aim of the ePD, namely to protect user privacy. • Instead, it risks: (i); (iii) further increasing the number of

	day-to-day online interactions which require consent, increasing consent fatigue and reducing user engagement with genuine tracking technologies; (ii) further degrading the online experience of EU users, who could be forced to make unrealistic 'consent' choices about critical processes in the online ecosystem; and (iii) an almost complete overlap between ePrivacy and GDPR for any personal data collected in an online environment. Crucially, this undermines the GDPR's purpose limitation principle, which would otherwise enable the onward processing of this data for compatible purposes.

DATA ACT

SIMPLIFICATION #1- Narrow the Scope of the definition of "Connected Product"	
Suggested change	Justification
Potential Change 1: Exclude a range of hardware products from scope of the DA by amending Article 2(5) *(5) 'connected product' means an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user, but shall not include products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service. Such products include, for example, personal computers, tablets, smartphones and smartwatches.*	• **Potential Change 1** seeks to exclude a range of products from the DA's scope, with the aim of reducing the compliance burden placed on organisations for these categories of product. Google notes that Recital (15) to the Commission's initial proposal for the DA contained such a carve-out and we have drafted this change on this basis. • The intention of the DA was to enhance the EU's data economy and foster a competitive data market by making data (in particular industrial data) more accessible and usable, encouraging data-driven innovation and increasing data availability. In practice, however, the broadly scoped nature of the DA's obligations is hampering innovation by placing organisations under significant burdens to comply

	with unclear rules that in certain cases conflict with other legal EU regimes (see further in Simplification #2). This change aims to reduce that compliance burden by narrowing the DA's scope.
[As a Fallback to the above] ***Potential Change 2: Exclude smartphones only from the Scope of the DA by amending Article 2(5)*** *(5) 'connected product' means an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user, but shall not include a smartphone.* **New Definition of Smartphone in Article 2 DA:** *'smartphone' means a mobile phone (as defined inas defined in Article 2(1) Regulation (EU) 2023/1670), which has the following characteristics:* *(a) it is characterised by wireless network connection, mobile use of internet services, an operating system optimised for handheld use and the ability to accept original and third-party software applications; and* *(b) it has an integrated touch screen display.*	• As a fallback to the above, **Potential Change 2** seeks to narrow the definition of connected product by excluding smartphones from its scope. Smartphones are a category of "connected product" that have the potential to significantly expand the DA's scope because of the potential for a wide range of apps to qualify as "related services" to a smartphone. • As a result, this simple change could significantly reduce compliance burdens for organisations by clarifying that the type of "connected products" and "related services" for which Google and other organisations must build DA-related compliance solutions does not extend to smartphones and their related services (i.e. apps).

SIMPLIFICATION #2 - *Carve out from Chapter II's scope data generated through the use of connected products/related services by consumers*	
Suggested change	Justification
Potential Change 1.1 - Targeted Amendment to Article 7 DA to narrow the scope of Chapter II to exclude consumer data ***Chapter II*** ***~~BUSINESS TO CONSUMER AND~~ BUSINESS TO BUSINESS DATA SHARING*** [..] *Article 7* ***Scope of ~~business-to-consumer and~~ business-to-business data sharing obligations*** *1. The obligations of this Chapter shall not apply to:* *(a) data generated through the use of connected products by consumers or related services provided to consumers.* *(b) data generated through the use of connected products manufactured or designed or related services provided by a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and*	• **Potential Change 1** proposes a targeted amendment to Article 7 DA that seeks to exempt from Chapter II data generated by the use of connected products and related services by consumers. • The effect of such an amendment is that only data generated through the use of connected/related services in a B2B context would be in scope of the Chapter II portability and information requirements, In addition, pre-contractual information would only need to be provided in a B2B context. The rationale for this change is that the GDPR/DMA adequately give effect to the right of data portability for consumer uses of connected products/related services, and it is therefore unnecessary and unduly burdensome to impose on organisations duplicative obligations to give effect to portability under the DA. • The same applies for the pre-contractual information obligations under Article 3(2)/(3), which overlap with the GDPR and are likely to overburden consumer users with additional (but very similar) disclosures. The average user is unlikely to understand the distinction between the disclosures made under GDPR and the DA. • Finally, carving out data generated by consumer products (which in many cases will be personal data) from the scope

where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service. *manufactured or designed or related services provided by a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service.* ~~*The same shall apply to*~~ *(c) data generated through the use of connected products manufactured by or related services provided by an enterprise that has qualified as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise.* *2. Any contractual term which, to the detriment of the user, excludes the application of, derogates from or varies the effect of the user's rights under this Chapter shall not be binding on the user.*	of the data portability obligations in Chapter II, aims to mitigate the risk assumed by data holders for GDPR non-compliance.
[[As a Fallback to Potential Change 1.1 ***Potential Change 1.2. Targeted Amendment to Article 7 to exclude data that is not useful for the recipient or the user*** *The obligations of this Chapter shall not apply to:*	• This potential change aims to introduce an exemption to the obligation to provide data portability under Chapter II DA in circumstances where the relevant data is not intelligible/would not be of any practical use to the recipient/user. At present, a significant portion of the data that data holders may be required to produce under

(a) data generated through the use of connected products and related services that is held by a data holder in a form that is not intelligible such that its disclosure would be of no practical benefit to the recipient or the user.	Chapter II will not be comprehensible/intelligible to users/recipients and its production will therefore be of little practical use to them. Despite this, data holders must still expend resources in creating solutions that permit the production of this data. This change aims to reduce the burden imposed on data holders by this obligation.

In addition to the above] Potential Change 2: Remove the Prohibition on Gatekeepers in A5(3) *3. Any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925, ~~shall not be an eligible third party under this Article and therefore~~ shall not:* *(a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1);* *(b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;* *~~(c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).~~*	• **Potential Change 2** seeks to remove the outright prohibition on "gatekeepers" under the DMA from receiving data under Article 5(3) DA. This prohibition creates significant legal uncertainty because of its potential conflict with Articles 20 GDPR/Article 6(9)/6(10) DMA. • In any case, an outright prohibition is inappropriate because there may be circumstances where users wish to transfer data to a gatekeeper. The aims of the provisions can be effectively achieved by prohibiting gatekeepers from soliciting such data. See further submissions made by the CCIA to the EC and EDPB.

SIMPLIFICATION #3 - *Confine the Chapter V Business to Government (B2G) Data-Sharing Obligations to Product Data and Related Service Data*	
Suggested change	Justification
Potential Change 1: Confine *Article 14* ***Obligation to make data available on the basis of an exceptional need*** *Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates an exceptional need, as set out in Article 15, to use certain product data and/or related service data, including the relevant metadata necessary to interpret and use those data, to carry out its statutory duties in the public interest, data holders that are legal persons, other than public sectors bodies, which hold those data shall make them available upon a duly reasoned request.* *Article 15* ***Exceptional need to use data*** *1. An exceptional need to use certain product data and/or related service data within the meaning of this Chapter shall be limited in time and scope and shall be considered to exist only in any of the following circumstances:* *(a) where the data requested is necessary to respond to a public emergency and the public sector body, the Commission, the*	• **Potential Change 1** seeks to limit the application of Chapter V B2G data-sharing obligations to product data (as defined in Article 2(15)) and related service data (as defined in Article 2(16))**.** This change aims to have the dual effect of (i) providing clarity and certainty on the scope of the Chapter V requests, and (ii) limiting the subject of those requests to product data and related service data. • This change aims to significantly reduce the operational burden on Google in ingesting and responding to requests, as systems and processes could be built within in-scope PAs to allow streamlining of the process.

European Central Bank or the Union body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions; *(b) in circumstances not covered by point (a) and only insofar as non-personal data is concerned, where:* *(i) a public sector body, the Commission, the European Central Bank or a Union body is acting on the basis of Union or national law and has identified specific product data and/or related service data, the lack of which prevents it from fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency; and* *(ii) the public sector body, the Commission, the European Central Bank or the Union body has exhausted all other means at its disposal to obtain such product data and/or related service data, including purchase of non-personal data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data.* *2. Paragraph 1, point (b), shall not apply to microenterprises and small enterprises.* *3. The obligation to demonstrate that the public sector body was unable to obtain non-personal data by purchasing them on the market shall not apply where the specific task carried out in the public interest is the production of official statistics and where the purchase of such data is not allowed by national law.*	

<u>Potential Change 2: Create a prescribed list of entities that can make requests under Chapter V</u> *Article 2(27)* *'Union bodies' means the Union bodies, offices and agencies prescribed by the Commission pursuant to Article 23(1), having been set up by or pursuant to acts adopted on the basis of the Treaty on European Union, the TFEU or the Treaty establishing the European Atomic Energy Community;* *Article 2(28)* *'public sector body' means the bodies designated as such by the Member States, pursuant to Article 23(2), being national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies (where designated as such by the Member States);* *Article 23* *1. The Commission shall be responsible for prescribing entities as 'Union bodies' within the meaning of Article 2(27), and maintaining a list of those Union bodies.* *2. Member States shall be responsible for prescribing entities as 'public sector bodies' within the meaning of Article 2(28), and maintaining a list of those public sector bodies.*	• **Potential Change 2:** This change seeks to require the Commission and Member States to produce and maintain lists of entities that may make requests under Chapter V. • This aims to provide clarity and prevent data holders from being overwhelmed by requests from multiple entities that do not have the right to make requests under Chapter V.