

Proposal for clearer wording of Article 88a/b Digitaler Omnibus

Ensuring informed data protection choices and fair competition

Version History

Version	Date	Change	Adapted by
0.0	ePrivacy Regulation	preliminary considerations	MvG
1.0	2nd June 2026	draft Art. 88b	MvG→multi-stakeholder feedback
2.0	3th July 2026	draft Art. 88a, changes Art. 88b	MvG
2.1	6th July 2026	editorial adjustments	MvG
2.2	31st July 2026	added visual examples / minor editorial adjustments / clarifications regarding content: • 88a(4)e (certification) • 88b(1)a and (8) sent. 2 (listed providers of automated means) • 88b(1)b/c (specific consent) • 88b(1)e (choice record and receipt) • 88b(3) sent. 2 (data subject rights wrt personalised content) • 88b(5) sect. 1 (specification „navigator.consent“) • 88b(5) sect. 2 (SMUs) • 88b(7) (data protection by design, Art. 25 GDPR)	MvG

Date:
6th July 2026

Author:

Prof. Dr. Max von Grafenstein, LL.M.

Affiliations:

University of the Arts Berlin (UdK)

Einstein Center Digital Future (ECDF)

Alexander von Humboldt Institute for Internet and Society (HIIG)

Table of content

Version History	0
Table of content	1
Intro: Enabling informed choices and fair competition	2
The current problem of uninformed choices and unfair competition	2
Ensuring informedness and fair competition by structuring choices as a process through a level playing field	3
Automatic choices as only known means in research and practice	3
More flexibility for opt-in/opt-out processes depending on the data protection risks	3
Effective communication of data protection risks through a common framework	4
Clarifying terms: Presettings, consent and objection, contextual request, handover notice	4
Different rules for respecting signals from choice agents	6
Current state of technology (highest readiness level)	7
Economic impact	8
General economic impact	8
Higher consent rates and lower bounce rates, especially for responsible business	8
Increasing user trust and consent rates, especially over time	9
Important note: Informed control depends on the specific visual design	10
Fair competition with respect to the implementation of choice mechanisms	11
Higher trust in efficiency of the rule of law	11
Stakeholder group-specific economic impact	12
Websites without marketing interests	12
Media service providers	12
Advertisers (e.g. online retailers and brands)	12
Third party providers (e.g. AdTech)	13
Consumers	13
Proposal for Article 88a (track changes and explanations)	14
Proposal for Article 88b (track changes and explanations)	19
Research background and institutions	34
Annex 1: Additional sales channel for publishers	35
Annex 2: Solving the issue with Apple's ATT	37

Intro: Enabling informed choices and fair competition

The current EC proposal for Article 88a/b Digital Omnibus aims at solving the problem of ineffective privacy choices, such as consent. The clarification of Article 88a/b proposed here aims to ensure that its regulatory objective is achieved: to enable consumers to make informed choices and to provide responsible businesses with the competitive advantage.

The current problem of uninformed choices and unfair competition

The current implementation of privacy choices, such as 'informed consent', does not allow for either informed or unambiguous decisions regarding the use of their data.¹ Although data subjects prefer privacy-friendly services to those with higher privacy risks, they are unable to identify these services or make choices in line with their privacy preferences.²

This lack of transparency leads to unfair competitive advantages for services with high data protection risks, as they receive the same consent rates as privacy-friendly services, whilst undermining data subjects' trust in all digital services and the effectiveness of law.

Reasons for the currently ineffective implementation of data protection choices include the

- bad timing (data subjects want to use the service rather than read the small print) and overwhelming amount of information presented in a small pop-up window;
- the repetition of the same information and options across a wide range of services;
- a complete lack of oversight of both the choices made across the services used and any changes that have occurred since the last use during repeat visits.

The current legal framework also means that the same requirements are imposed on users' decisions for different processing operations, regardless of the extent of the respective data protection risk. This, too, leads to fatigue amongst users, who click away every prompt without understanding the different consequences for themselves.

¹ See, for example, Utz, C., Degeling, M., Fahl, M., Schaub, F., and Holz, T. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 973–990. <https://doi.org/10.1145/3319535.3354212>; Bielova, Nataliia et al., The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions, in: Proceedings of the 33rd USENIX Security Symposium (USENIX Security '24), 2024; Santos, Cristiana / Rossi, Arianna / Sánchez Chamorro, Lorena / Bongard-Blanchy, Kerstin / Abu-Salma, Ruba, Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens, arXiv:2110.02597, 2021; Grassl, P., Gerber, N., & Grafenstein, M. v. (2024). How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights? European Data Protection Law Review, 10(1), 96-104. DOI: 10.21552/edpl/2024/1/14.

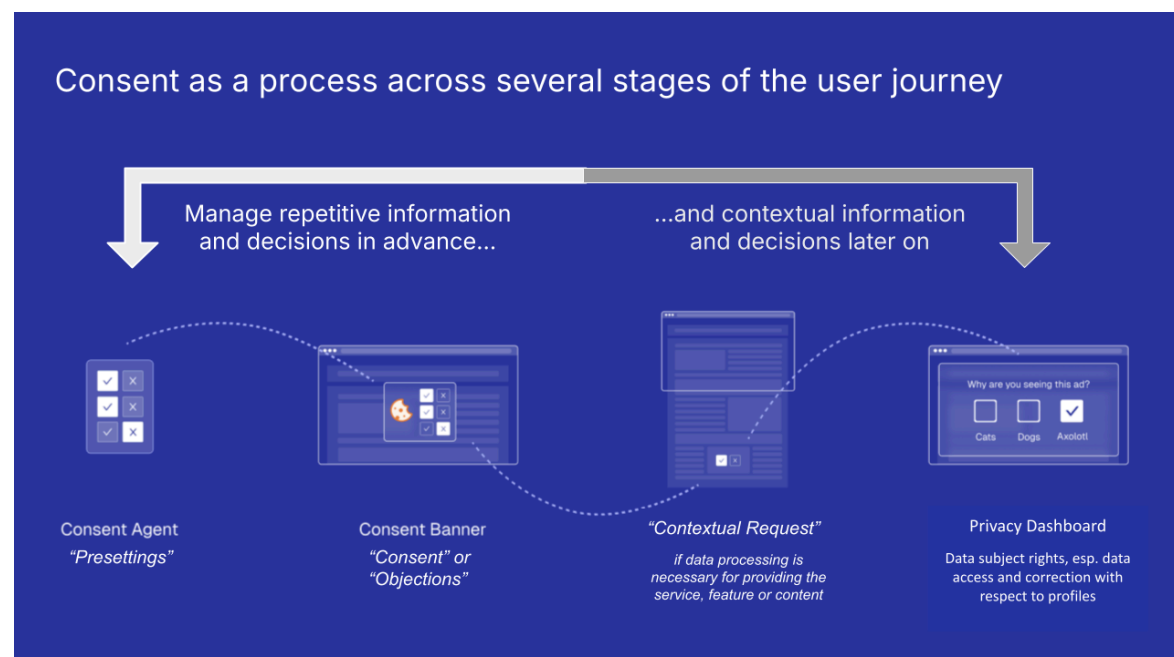
² See, for example, Tsai, J. Y., Egelman, S., Cranor, L., Acquisti, A. The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study. Information Systems Research Vol. 22, No. 2, June 2011, pp. 254–268.

Ensuring informedness and fair competition by structuring choices as a process through a level playing field

Agent-enabled choices as only known means for effective privacy decisions

These issues are resolved by embedding the information and decision-making options more user-friendly into the respective phase of the user journey on the basis of a choice agent. To reduce the cognitive overload on data subjects, they must be enabled to

- **manage recurring information and decision options in advance** so that when using a service they can focus on the differences adjusting their pre-settings;
- **focus on** specific services, features or content in **the relevant usage context** because it enables them to better understand the significance of a request; and finally,
- always **maintain an overview of all their decisions** made across the services and any changes that have occurred since the last use during repeat visits.



In both academic research and practical application, there are currently no known alternatives to solving the problem other than through choice agents. Provided that the law grants those affected the opportunity to make their own decisions in the first place.

More flexibility for opt-in/opt-out processes depending on the data protection risks

The approach proposed here also advocates making the requirements regarding the user choices more flexible, depending on the data protection risks caused by the processing. The proposal therefore includes a further legal basis for the legitimate interests of service providers in the form of a new Article 88a(3)(e). However, a service provider may only rely on this legal basis if data subjects are able to object in every case; furthermore, the

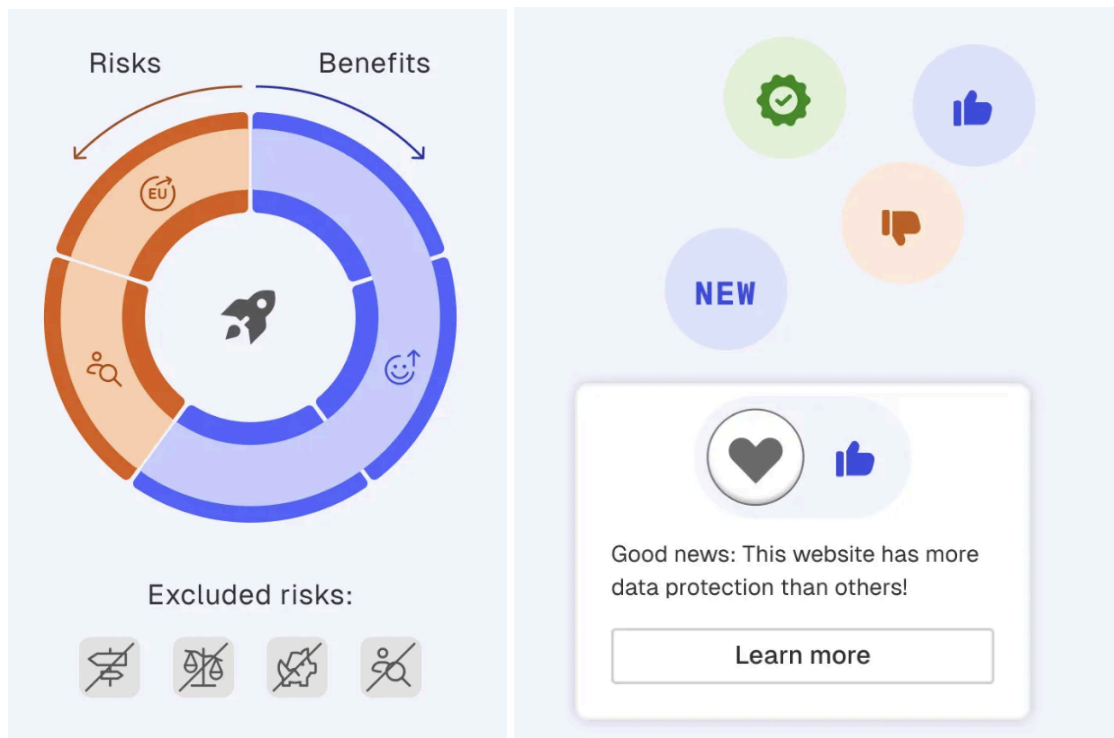
provider must ensure that the relevant processing operation is subject to a code of conduct, according to Article 40 GDPR, or have it certified, according to Article 42 GDPR.

However, it should be noted that this increased flexibility does not in itself solve the problem of uninformed decisions, as decisions still have to be made. The requirement in Article 88b that service providers must respect the signals from choice agents therefore also applies to the right to object.

Effective communication of data protection risks through a common framework

This proposal establishes a common framework for how decision-making options for data subjects must be implemented, taking into account the respective data protection risks associated with the processing operations. Such a level playing field

- enables data subjects to make their own decisions in light of the respective data protection risks;
- enables responsible companies to finally communicate their high standards of data protection effectively to data subjects through this transparency;
- at the same time, it prevents unfair practices in the implementation of decision-making mechanisms, which have previously allowed certain parties to gain an unfair competitive advantage (see the example of Apple's App Tracking Transparency Framework (ATT) in Annex 2).



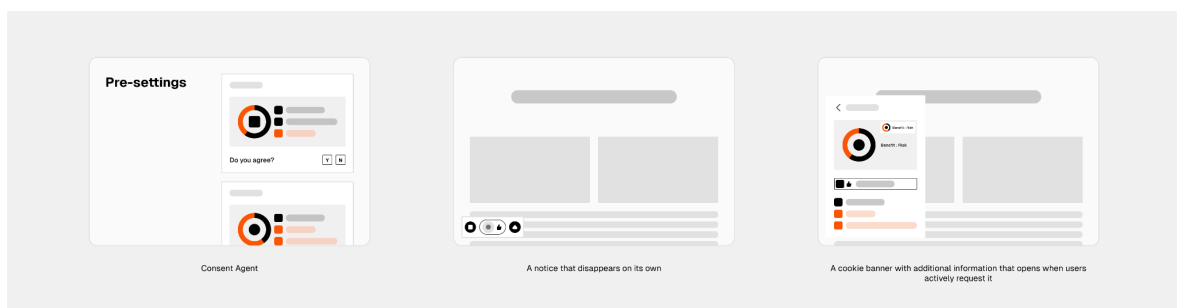
Left-hand example: Risk/benefit ratio

Right-hand example: Handover notice

Clarifying terms: Presettings, consent and objection, contextual request, handover notice

According to the refined understanding of choice as a process, there are several types (or steps) of decision making-elements:

- The term '**presettings**' refers to an explicit but general default setting that a user configures in a choice agent, but which they can adjust when using a specific service, feature or content through a so-called handover notice;
- The term "**handover notice**" refers to a visual interface that disappears automatically after a reasonable period of time, which is displayed to users of a choice agent in place of the traditional cookie banner, and which allows users to adapt their pre-settings from their agent to the specific service being used; via the handover notice, users can open the traditional cookie banner to obtain further information on data processing.
- The terms '**consent**' and '**objection**' refer to a user's decision to allow their data to be shared for a purpose which, whilst related to the use of the specific service, *is not necessary* for the requested service, function or content.
- The term '**contextual request**' refers to a situation in which a user requests a specific service, function or content for which the processing of their data *is necessary*.

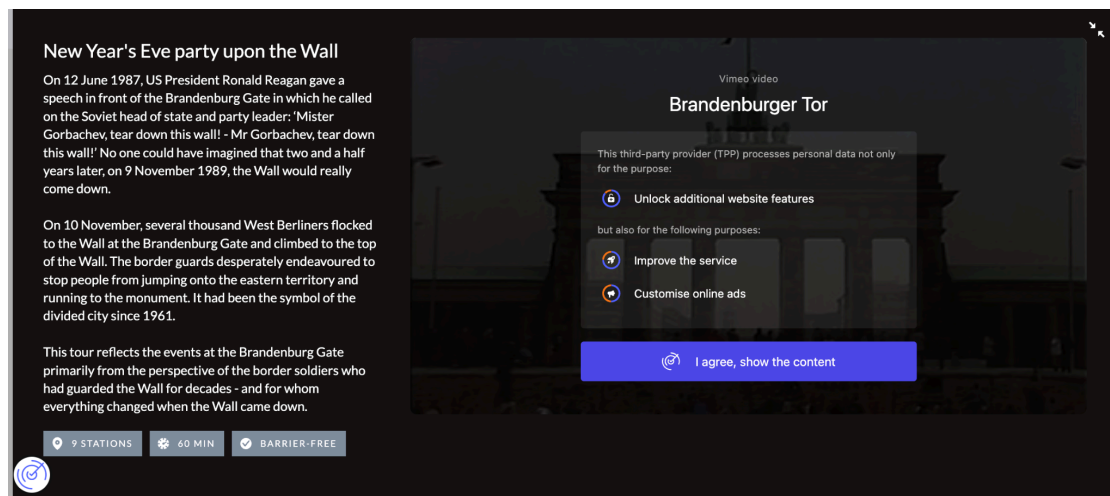


"Contextual requests" for services, features or content

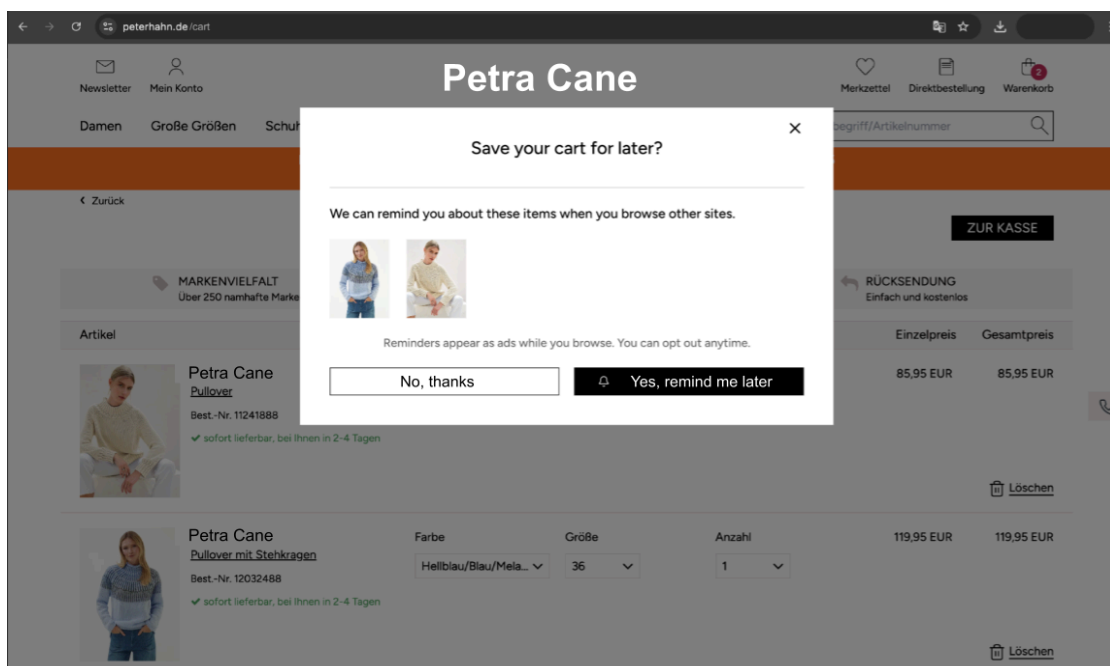
'Contextual requests' may relate not only to a service as a whole (e.g. displaying a website), but also to specific content (e.g. a map or a video) or a specific function (e.g. the personalisation of the service or part thereof); from the user's perspective, the point is that the use of the *requested service*, feature or content technically necessitates the processing of their data; whilst they can decline to give *consent* or object to the processing of their data without this making the provision of the service, feature or content technically impossible (in contrast, with a 'Pay-or-Okay' banner, a service provider prevents its use for economic reasons; see below for further details).

The first example below shows that the 'contextual request' to display the video relates only to the first processing purpose listed ('Unlock additional website feature'), as it is only

here that the processing of the data is technically necessary. By contrast, the processing of data to 'improve the service' or to 'customise online ads' is not technically necessary for the video to play and can therefore only be legitimised by 'consent' in this usage situation.



In contrast, the second example shows a reminder function in an online shop and, thus, a marketing measure. Nevertheless, given the specific context of use, the processing must be regarded as necessary. The feature is displayed to the shop visitor because they have filled their shopping basket but wish to leave the website without completing the purchase. As this feature arises directly from the context of the online shop visitor's use of the site, the processing of the data is to be regarded as technically necessary for the fulfilment of the reminder feature, provided the visitor explicitly requests the feature. Although the 'remember me' function in the online shop is a marketing feature, the processing of data in this second example is necessary, whereas the data processing for advertising purposes in the first example was not necessary simply because the context of use is different.



These two examples show that, from the user's perspective, it depends largely on the specific context of use as to whether the processing of their data is necessary for a particular feature or not – and whether their decision to share their data should be regarded as 'consent' or a 'contextual request' for a service, and what legal consequences should be attached to it.

Different rules for respecting signals from choice agents

The problems mentioned above – i.e. 'click fatigue', uninformed and ambiguous choices, and the lack of an overview of which choices a user has made in relation to which service – occur with respect to the three decision types: **consents, objections, and contextual requests**. However, services must respect signals from choice agents and communicate with them to varying degrees depending on the specific decision type.

- **Respect regardless of a “yes” or “no”:** With regard to “consents” and “options to object”, service providers must respect the pre-settings a user has configured in their consent agent, regardless of whether these constitute consent, refusal or an objection. This means that providers must not hinder or interrupt the use of their service in order to thereby force the user to make an additional active decision. The service provider may only display a so-called 'handover notice', which enables the user to adapt their respective default settings to the specific circumstances of the service. However, this handover notice disappears automatically after a reasonable period of time, without the user being forced to take any further action.
- **Respect only in the case of “yes”:** In the case of a 'contextual request', in contrast, the provider needs only to 'respect' an *affirmative* pre-setting by the user from their agent. The provider may hence provide the service, function or content without the user having to make another active click. If, on the other hand, no affirmative pre-setting has been given, the service, feature or content cannot function without data transmission *for technical reasons*. The user is thus obliged to make a further active decision if they wish to use the service, feature or content.

Important note: Whilst choice agents solve the problem of click fatigue and uninformed choices by bringing recurring information and settings to the fore and centralising them, contextual requests primarily address the issue by embedding the decision within the actual context of use of the service, feature or content. Contextual requests are therefore not primarily about avoiding choices altogether, but rather about offering them in a more user-friendly way.

- **Ongoing monitoring and adjustment options:** For all three types of decision, the service and choice agent providers must provide for the following functions:
 - Choice agents must provide end users for an overview of all their decisions relating to every service they have visited so far.

My Consents

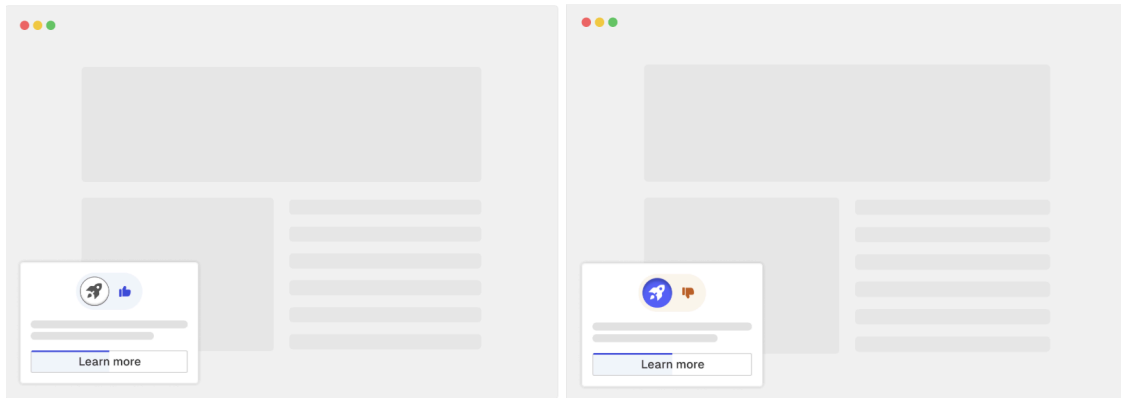
Keep track of your given consents and adjust them anytime if you like.

🔍 Search by domain names

02/01/2025

● domain.com	   
averyveryverylooongurl.com	You denied all purposes for this site
● anotherexamplewebsitetwo.com	   
01/01/2025	
● websitethree.com	   
alooongurl.com	You denied all purposes for this site

- Service providers must enable end users to adjust their decisions on subsequent visits if the risks have changed since their last visit (as the risks communicated form the basis for end-users' decisions).
 - In the case of 'contextual requests', this is done via a small visual indicator directly next to the service, function or content in question; through this indicator, the end user may open the cookie banner, get more details and adjust their decisions if they want.
 - In the case of 'consents' and 'objections', the service provider must show a handover notice (automatically self-disappearing after a certain period of time) enabling the end user to see first information on the changed risk, open the cookie banner to get more details and/or adjust their decisions if they want.



To this end, providers must synchronise the user decisions stored on their systems with their agent, across repeat visits.

Current state of technology (highest readiness level)

It is important to clarify that the technical system for implementing the approach proposed here has been fully developed and broadly tested in practice (see the Consenter research demonstrator, available at www.consenter.eu/).

The technical, organisational, visual and legal specifications are freely available under the Creative Commons CC-BY-ND licence; all techniques for the reproduction and further improvement of the consent mechanisms proposed here are available under the Creative Commons CC-BY-SA licence (see under <https://www.consenter.eu/about/open-access>).

The methods for demonstrating the effectiveness of the techniques proposed here, within the meaning of Articles 25 and 32 of the GDPR, have been published in peer-reviewed scientific journals, mostly under open access licences (see www.consenter.eu/de/about/approach).

Economic impact

Once data subjects understand the data protection risks resulting from their use of a service, they can adjust their decisions accordingly. This creates, for the first time, the

promised competitive advantage for data protection-friendly services, as they can distinguish themselves positively from services with higher risks.³

General economic impact

Higher consent rates and lower bounce rates, especially for responsible business

Studies show that the more trustworthy a service is – and, in particular, the lower the data protection risks – the higher the consent rate (compare, in the table below, the cross-purpose and risk-independent consent rates in study group 1, which used a status-quo cookie banner, with the purpose- and risk-dependent consent rates in study group 3, which made their choices with the help of a consent agent).⁴



Grafenstein, M. v., Herbolt, N., REGULATION OF ONLINE ADVERTISING. Expert Report. 20. December 2024. Federation of German Consumer Organisations (vzbv)

There are numerous qualitative indicators suggesting that effectively communicating low data protection risks also reduces the bounce rate (i.e. the number of users who leave a service because they find the display of a cookie banner too intrusive) and the objection rate (provided that users have been offered an effective means to object in the first place).

³ See the summaries of the empirical research on the economic effects at and the state of the art in the visual design of choice architectures at www.consenter.eu under Resources, in particular, the summary of current research results on the behavioral and economic effects of consent agents at <https://tinyurl.com/Art88b-Fair-Competition>.

⁴ Grafenstein, M. v., Herbolt, N., REGULATION OF ONLINE ADVERTISING. Expert Report. 20. December 2024. Federation of German Consumer Organisations (vzbv), pp. 123 et seq.; V. Grafenstein, Effective regulation through design: Cookie Pledge, Do Not Track... How Is All That Supposed To Work From A User's Point Of View?, SSRN 2024, p. 41 (the full paper is currently in review).

These positive effects apply in particular to providers who have already invested considerable effort in designing their services to be privacy-friendly, but who were so far unable, due to the currently opaque system, to communicate the reduced risks effectively.

Increasing user trust and consent rates, especially over time

Responsible companies will also be able to continuously increase consent rates over time. The reason for this is that the general level of trust amongst consumers is very low due to the current design of the cookie banner.⁵ If choice mechanisms are designed in such a way that leads to more informed choices and more effective control by data subjects, their trust in the disclosure and processing of their data is going to increase.⁶

One key mechanism for this purpose is the so-called risk monitoring aka. trigger system. It provides service providers with an incentive to continually reduce data protection risks: In general, if users declined to give their consent or objected to data processing during their last visit, the service provider must not ask them to make a decision again the next time they use the service (to avoid 'click fatigue'). However, if the service provider has been able to reduce the risks since the last visit, users are presented with a new basis for decision-making, meaning they may – and must – be asked again; the same applies in reverse (see Article 88b(3) first subparagraph).⁷

Another mechanism for continuously increasing trust are the preference centres/privacy dashboards, which facilitate the other data subject rights, such as user-friendly control over their advertising profiles (see our proposal in Article 88b(3), second subparagraph). Studies show that, thanks to the user-friendly transparency and control features of such dashboards, users gain a much better understanding of data processing and develop significantly greater trust in it.⁸

Important note: Informed control depends on the specific visual design

Users' awareness and effective control depend decisively on the specific design of the agent-based choice mechanisms. For this reason, the study commissioned by Google, 'Gone in One Click', is highly misleading, as it takes Apple's App Tracking Transparency

⁵ See the results from a quantitative survey conducted by the German Federal Data Protection Commissioner (Bundesdatenschutzbeauftragte) available at https://www.bfdi.bund.de/DE/BfDI/Datenbarometer/Cookies-PIMS/Cookies-PIMS_node.html (last re-call 6th July 2026).

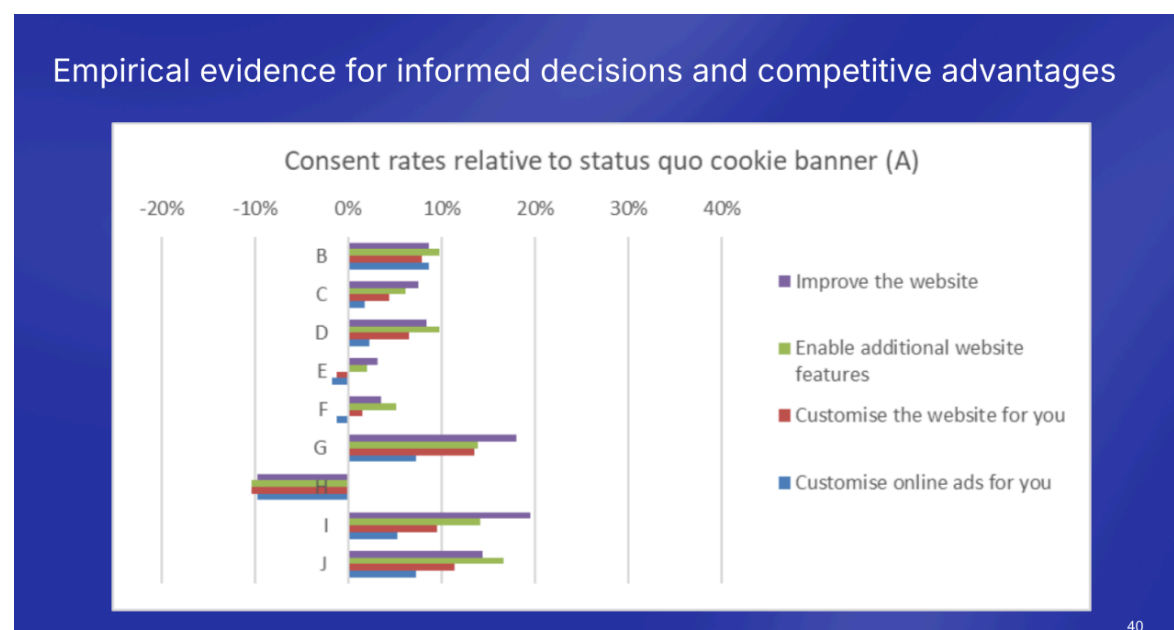
⁶ Smieskol, P., Jakobi, T., & von Grafenstein, M. (2025). From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalized and non-personalized content through an On/Off toggle. *Computer Law & Security Review*, 59, 1-22. DOI: 10.1016/j.clsr.2025.106186.

⁷ See also the freely available visualisation examples from the Consenter research demonstrator, available in the documentation at <https://documentation.consenter.eu/maintenance>.

⁸ See the 'Secure in Data Traffic' research and development project, in which the consortium partners, together with, amongst others, The German Association for the Digital Economy (BVDW), are developing a corresponding research demonstrator, more information at <https://sid-projekt.de/> (last re-call 6th July); see the 'single interface' recommended in the Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – Final report, commissioned by the European Commission, pp. 261/262.

(ATT) framework as the basis for its extrapolation – and thus presents a negative example of how choice mechanisms should not be designed, and what Articles 88a/b are actually intended to prevent.⁹

If agent-based choice mechanisms are designed not simply to make it as easy as possible to either consent to or decline data processing, but to enable genuinely informed decisions, the consent rate is, in any case, up to 20 % higher than with current cookie banners designed in accordance with best practice guidelines. The following chart takes the consent rate for such a ‘best practice’ cookie banner as its starting point and illustrates the differences in consent rates resulting from the various designs. The lower consent rate in Group H is due to a design that is structurally similar to Apple’s ATT (i.e. featuring a double opt-in mechanism).



publication in progress

Fair competition with respect to the implementation of choice mechanisms

Articles 88a and 88b also ensure a level playing field by setting out specific conditions for the implementation of informed decisions. At present, services that pose high data protection risks to users gain an unfair competitive advantage because, due to the current lack of transparency, they generally achieve the same consent rates as data protection-friendly services – even though users actually prefer privacy-friendly services.

Furthermore, very large online platforms use their power by providing choice mechanisms in a way that disadvantages their competitors. One example is Apple’s App Tracking Transparency Framework (ATT), which has led to a significant reduction in consent rates among providers of iOS and macOS apps. Another example is Google’s Third-Party

⁹ See the study commissioned by Google, available at <https://tinyurl.com/GoneInOneClick> (last re-call 6th July 2026); contrary to this study, Informed consent as a key to fair competition: How to turn data protection into a competitive advantage with consent agents, available at <https://tinyurl.com/Art88b-FairCompetition> (last re-call 6th July 2026).

Phase-Out Initiative, as part of their Privacy Sandbox, which sought to introduce a similar mechanism; Google abandoned the initiative only under pressure from competition authorities and competitors. A further example is the implementation of the right to object to the processing of personal data for the purpose of AI training. Here, some platforms, like Meta and LinkedIn, have concealed this option to such an extent that users are unable to effectively exercise their right to object.

As these practices arise directly from the way in which choice mechanisms are designed, they must be regulated in direct connection with the requirements governing such choices.

Higher trust in efficiency of the rule of law

Last but not least, Articles 88a/b also serve to restore trust in the effectiveness and efficiency of the rule of law. The vast majority of stakeholders are aware that the current implementation of the cookie banner is not only ineffective, but also inefficient. Most stakeholders blame the regulation for this. By specifying the implementation of effective and efficient choice mechanisms, the legislator proves them otherwise.

Stakeholder group-specific economic impact

Websites without marketing interests

Positive impact

- higher consent rates than with the current status quo cookie banner, due to the processing purposes posing fewer data protection risks
- greater user trust in the website and the organisation behind it

Negative impact

- None (apart from the very low cost of switching to a different banner design)

Media service providers

Positive impact

- additional sales channels if cooperation with choice-agents (see the visual example in Annex 1)
- strengthened trust relationship between users and media services (important in view of AI agents, which will increasingly challenge this individual interaction)
- as soon as preference centre/privacy dashboard gets integrated (which gives users effective control over their advertising profile):
 - lower bounce rates than with the current status quo pay-or-okay banner, due to higher trust in the data processing for ads purposes

- higher data quality since users are able to adjust their ads interests

Negative impact

- None, as they continue to display their 'pay or okay' banner (see Article 88b(3))
- Implementation costs low, though slightly higher with preference/privacy dashboard

Advertisers (e.g. online retailers and brands)

Positive impact

- higher consent rates in iOS and macOS apps, as Article 88b requires Apple to integrate the more user-friendly process (instead of ATT – see Annex 2)
- higher contextual-request rates, as users are more successfully convinced of a positive risk-benefit ratio when engaging with content from the retailer or brand
- as soon as preference centre/privacy dashboard gets integrated (which gives users effective control over their advertising profile):
 - additionally increasing consent and contextual request rates, due to higher trust in the data processing for ads purposes
 - higher data quality since users are able to adjust their ads interests

Negative impact

- Potentially lower *consent* rates are offset in the short term by higher *contextual request* rates and overcompensated in the medium to long term, due to better understanding of positive risk/benefit ratio and higher trust
- Implementation costs low, though slightly higher with preference/privacy dashboard

Third party providers (e.g. AdTech)

Positive impact

- increased demand for privacy-friendly providers due to the greater transparency of product quality and the aforementioned benefits for their business customers

Negative impact

- decreased demand only for privacy-unfriendly providers due to disadvantages for their business customers when using privacy-unfriendly services

Consumers

Positive impact

- significant time savings¹⁰
- using services or providing their data to services that they actually trust and prefer

Negative impact

- None

¹⁰ Farronato, Chiara / Fradkin, Andrey / Lin, Tesary, Designing Consent: Choice Architecture and Consumer Welfare in Data Sharing, NBER Working Paper No. 34025, 2025, available at <https://www.nber.org/papers/w34025>; Demir, Nurullah / Urban, Tobias / Pohlmann, Norbert / Wressnegger, Christian, A Large-Scale Study of Cookie Banner Interaction Tools and Their Impact on Users' Privacy, Proceedings on Privacy Enhancing Technologies (PoPETS), Vol. 2024, No. 1, 2024, S. 5–20, DOI: 10.56553/POPETS-2024-0002; Devergranne, Alexandre, Europeans Spend 575 Million Hours Clicking Cookie Banners Every Year, Legiscopes, 2026, available at <https://www.legiscopes.com/blog/hidden-productivity-drain-cookie-banners.html>; Advance Metrics, Cookie Behaviour Study, 2023, available at <https://www.advance-metrics.com/en/blog/cookie-behaviour-study/>; Farronato, Chiara / Fradkin, Andrey / Lin, Tesary, The Time Cost of Customizing Website Cookies, Visualized, Harvard Business School, Working Knowledge, 2025, available at <https://www.library.hbs.edu/working-knowledge/time-cost-of-customizing-website-cookies-visualized>.

Proposal for Article 88a (track changes¹¹ and explanations)

Article 88a

Processing of personal data in the terminal equipment of natural persons

(1) Storing of information, or gaining of access to information already stored, in the terminal equipment of a natural person ('data subject'), is regarded as 'personal data processing' in accordance with this Regulation. For the definition of the controller, Article 4(7) applies.

Clarification and reason:

The extended material scope of application to any information is in line with the ePrivacy Directive and avoids the question of whether or not this information relates to natural persons.

The addition in brackets 'data subjects' also makes it clear that these natural persons are to be treated as 'data subjects'. The same clarification applies to the 'controller'.

These amendments are applied throughout Articles 88a and 88b and are not further justified in the following.

(2) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a data subject~~natural person~~, and any subsequent processing necessary to achieve the purpose for which the data subject has given consent, is only allowed when that ~~data subject~~person has given his or her consent, in accordance with this Regulation.

Clarification and reason:

The addition of 'and any subsequent processing necessary to achieve the purpose for which the data subject has given consent' clarifies, in line with paragraph 3, that all further processing operations following 'storing' or 'gaining access' of that information may be based on the same consent, provided that they pursue the same purpose as that specified in the consent.

¹¹ The starting point is the European Commission's proposal; underlined words have been added to this proposal (though, there are a few purely formal clarifications which have not been underlined separately for the sake of readability), whilst words marked with a strikethrough should be deleted.

For the terminological distinction between ‘consent’ in paragraph 1 and ‘service request’ in paragraph 3(b) above, see above in the introduction ‘Clarifying terms: Presettings, consent and objection, contextual request, handover notice’. This distinction should be clarified in Article 4 (Definitions) and/or in the recitals.

(32) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).

(43) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a data subject ~~natural person~~ without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:

- (a) carrying out the transmission of an electronic communication over an electronic communications network;
- (b) providing a service, feature or content explicitly requested by the data subject (‘contextual request’);

Clarification and reason:

The legal basis for processing data at the data subject’s ‘request’ relates not only to a service as a whole, but also to a function or piece of content within a service.

This therefore also covers, for example, the activation of a video, a map or social media content embedded within a service. It also covers the personalisation of the service or part of the service, provided that the request arises directly from the context of use in which the personalisation is offered. Similarly, the sending of advertising is also covered, provided that the offer arises directly from the context of use, such as an offer to send a reminder if a data subject has filled their shopping basket but then leaves the website without completing the purchase (see above in the introduction ‘Clarifying terms: Presettings, consent and objection, contextual request, handover notice’).

In any case, the data subject must be able to withdraw the request just as easily as it was made – usually by toggling a button that can be accessed with a single click (see Article 88b(1)(a) in this regard).

For the terminological distinction between ‘consent’ in paragraph 1 and ‘contextual

request' in paragraph 3(b) above, see above in the introduction 'Clarifying terms: Presettings, consent and objection, contextual request, handover notice'. This distinction should be clarified in Article 4 (Definitions) and/or in the recitals.

(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;

(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service;

(e) 'legitimate interests' according to Article 6(1) lit. f provided that the data subject has the unconditional right to object to the processing of their data and that the processing operations carried out on the grounds of 'legitimate interests' are subject to a code of conduct in accordance with Article 40 or are certified in accordance with Article 42.

Clarification and reasons:

The approach proposed here advocates making the requirements regarding the user choices more flexible, depending on the data protection risk caused by the processing. The proposal therefore includes a further legal basis for the 'legitimate interests'.

However, a service provider may only rely on this legal basis if data subjects are able to object in every case. Thus, the aim of introducing greater flexibility is not to completely dispense with the data subject's right to choose, but rather to tailor the requirements for decision-making options to the risks involved. Only where the data protection risks are no greater than the 'legitimate interests' is an objection option (opt-out mechanism) sufficient; where the data protection risks outweigh the 'legitimate interests', consent (opt-in) is required.

The additional legal basis not only provides a legal and competitive advantage for responsible data controllers who pose low data protection risks. It also serves as an incentive to invest in privacy-preserving technologies (PETs), as these can, in principle, reduce data protection risks to such an extent that they no longer outweigh 'legitimate interests'.

Apart from the mandatory right to object, the data processor must ensure that the

processing in question is subject to a code of conduct in accordance with Article 40 of the GDPR, or have it certified in accordance with Article 42 of the GDPR. This means that the otherwise voluntary co-regulation options under Articles 40 and 42 become a mandatory requirement for the legal basis to be applicable.

This is intended to prevent data controllers from abusing the increased flexibility in view of the well-known shortcomings in enforcement by data protection authorities.

As the certification or code of conduct must relate to the processing operation and not to the processing entity (see the wording of Articles 40 et seq. GDPR), the adherence to a certification or code of conduct may be applied for and carried out not only by a controller (usually the service provider), but also by a data processor (usually the third-party provider).

The latter is particularly advisable in cases where the critical processing is carried out, from a technical and organisational perspective, by the processor. Furthermore, a processor benefits from significant economies of scale, as it can offer the same certified data processing service to a large number of controllers.

(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on sect. 1 or 3 lit. b or e ~~consent~~, the ~~following shall apply~~, the data subject shall be able to decline requests for consent (sect. 2) and contextual requests (sect. 4 lit. b), withdraw them as well as object to the data processing in an easy and intelligible manner with a single-click button or equivalent means.

~~(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;~~

~~(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.~~

~~This paragraph also applies to the subsequent processing of personal data based on consent.~~

Clarification:

The legal specifications for visual implementation have been extended to cover 'contextual requests' on the one hand, and the withdrawal of 'consent' and of 'contextual requests' on the other.

The provisions set out in lit. b and subsequent subparagraphs have been moved, for reasons of higher thematic proximity, to Article 88b (section 2 lit. b).

Reason:

In current practice, visual interfaces are often designed in such a way that it is not only difficult for the data subject to decline a consent request, but also difficult to withdraw consent and, above all, difficult to object to the processing of data. The latter has been demonstrated most recently by the visual design of interfaces for the processing of personal data for AI training, where the option to object was often hidden in such a way that it could only be found with very high effort.

(5) This Article shall apply as soon as Article 88b applies~~from [OP: please insert the date — 6 months following the date of entry into force of this Regulation].~~

Clarification and reason:

The greater flexibility provided for in Article 88a in favour of industry, compared with the current ePrivacy Directive, shall only apply if, in return, the problems of consent fatigue, uninformed decisions and a lack of overview of the decisions taken on the part of data subjects are resolved. This is intended to prevent cherry-picking by industry.

Proposal for Article 88b (track changes¹² and explanations)

Article 88b

Automated and machine-readable indications of data subject's choices ~~with respect to processing of personal data in the terminal equipment of natural persons~~

Clarification:

The proposal extends the use of automated and machine-readable means to all processing of personal data in respect of which data subjects are entitled to indicate a decision under data protection legislation, regardless of the data to which it refers and whether they are entitled to indicate that decision by means of consent, contextual requests, withdrawal, or objection.

Reason:

The problem of uninformed and ambiguous decisions exists not only in relation to the collection and processing of data concerning their terminal equipment, but everywhere. Server-side tracking, which does not rely on end devices, is a prime example of the problem of potentially opaque data processing operations and the corresponding lack of transparent and unambiguous consent.

Extending this to all decisions guaranteed under data protection law thus ensures that data subjects can consistently express their decisions through automated and machine-readable means, and that all kinds of (third-party) service providers have a level playing field with regard to all such decisions made by data subjects.

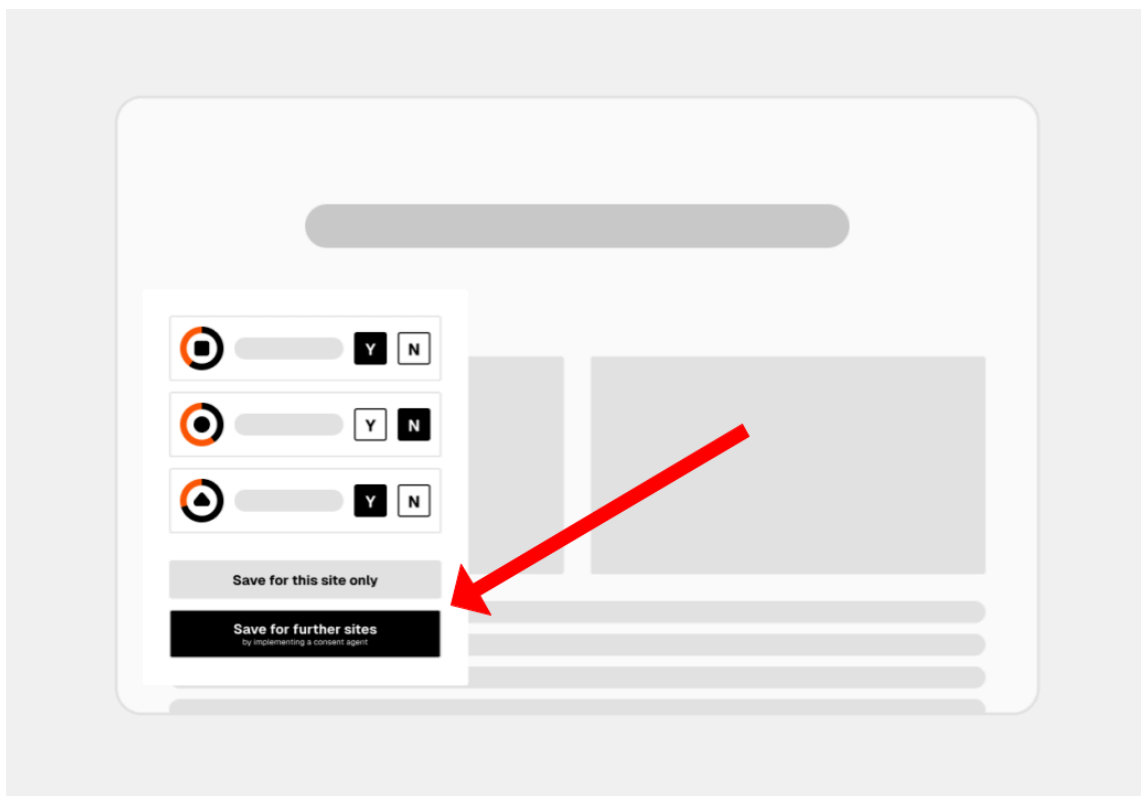
(1) Controllers shall ensure that their online interfaces allow data subjects to:

- (a) access, in an easy and intelligible manner with a single-click button, automated and machine-readable means through which they can give and withdraw consent and object to the processing of personal data; the single-click button must link to a website of the European Data Protection Board on which all providers of automated means are listed, in accordance with sect. 8 sent. 2.

¹² The starting point is the European Commission's proposal; underlined words have been added to this proposal (though, there are a few purely formal clarifications which have not been underlined separately for the sake of readability), whilst words marked with a strikethrough should be deleted.

Clarification:

This requirement ensures that data subjects can find and get a solution to the problem of uninformed and fatiguing decisions where the problem arises: in the classic cookie banner (see visual example below).



Reason:

If such an obligation did not exist, the solution of automated and machine-readable means would in all likelihood have no practical relevance, because too few data subjects would be aware of it.

It is also conceivable to include additional obligations, notices and links to automated and machine-readable resources (so-called ‘calls to action’), such as for browser providers when their users open the browser.

*Once there are several providers on the market offering automated and machine-readable means that comply with the standards set out in paragraph 7, the single-click button provided by service providers **must** link to a website of the European Data Protection Board, where all compliant services are listed. Data subjects can then select the service*

that best suits their needs from there.

(b) give consent and request a service, feature or content ('contextual request') through automated and machine-readable means, provided that the conditions for consent or contextual request laid down in this Regulation are fulfilled;

(c) decline a request for consent, withdraw consent and contextual request, and exercise the right to object pursuant to Article 21 and Article 88a sect. 4 lit. e(2) through automated and machine-readable means.

Clarification:

Article 88b and a shall explicitly clarify that it also extends to the automated exercise of the right to withdraw consent under Article 7 (3) and to object under Article 21 GDPR; the scope shall not be limited to objections under Article 21(2) GDPR.

Furthermore, the regulation must, in part, relate to contextual requests in accordance with Article 88a(4)(b). As highlighted in the introduction ('Different rules for respecting signals from choice agents'), the controller shall also respect an agent's affirmative signals in the case of contextual requests, to ensure the smoothest possible user experience. Conversely, this does not apply in the event of a negative pre-setting on the part of the agent, because the service, feature or content cannot technically be provided without data processing.

The recitals should also make it clear that the acceptance by a controller (usually a service provider) of consent given by automated means constitutes 'specific consent' within the meaning of Article 4 no. 11 GDPR.

Reason:

Although Article 21(5) GDPR already contains a provision comparable to Article 88b specifically for objections, the clarifying addition in Articles 88b/a ensures that the further requirements apply equally to both forms of choice, i.e. opt-in and opt-out.

This is important because both forms of choice complement one another both legally and from the data subject's perspective, provided that both are available in practice (see the new Article 88a(3) lit. e proposed here for 'legitimate interests').

The clarifying inclusion of the automated right to object in Articles 88b/a thus prevents inconsistencies in the normative structure and in the data subject's user experience. See the following specific requirements in this regard.

The clarification in the recitals regarding the sufficient specificity of consent given by automated means is intended to enhance legal certainty, as this has been the subject of debate for several years, particularly in Germany.

(e) automatically receive a record and receipt of their choice made.

Clarification:

This requirement ensures that data subjects receive a record of which services they have consented to and for what purpose, as well as which services they have not consented to, which services they have requested by means of a contextual request and which they have not, and when they have withdrawn their consent or objected to the processing of their data (see visual example in the introduction).

When storing this data, particular attention must be paid to compliance with the data protection principle of data minimisation and to the security of the processing.

Reason:

The provision implements a key prerequisite for an effective legal system, whereby all parties entering into a legal transaction are equally provided with evidence of its existence and contents or non-existence. Currently, only service providers receive such proof, not the data subjects. Consequently, data subjects have neither an overview of which decisions they have made regarding which service, nor are they in a position to substantiate one or the other in legal disputes.

(2) Controllers shall respect the choices made by data subjects through automated means ('pre-settings') in accordance with paragraph 1 lit. c and d, subject to the following conditions:

(a) when using the service for the first time via automated means, the data subject must, at the start of their use of the service, be able to adapt their decisions made by automated and machine-readable means to the specific circumstances of the

controller's service in a simple and understandable manner; the design of the button or equivalent means used to adjust the choices must disappear automatically after a reasonable period of time.

Clarification:

Data subjects should be able to adjust their default settings made through the automated means to suit the specific circumstances without being forced to click away a traditional cookie banner. In practice, this can be achieved by means of a visual interface that is displayed to the data subject at the start of their use of the service, but which then disappears automatically after a reasonable period of time (so-called handover notice, see the visual examples given in the introduction). The specific design must be tailored to the needs of the data subject and substantiated by appropriate empirical evidence (see paragraph 7 (b) below).

Reason:

Both data subjects and data controllers have a legitimate interest in ensuring that data subjects can adapt the pre-settings they have made via automated and machine-readable means to the specific service being used, right from the start of their use of the service. The reason for this is that data subjects essentially base their decisions on three factors:

- *the data subject's prior knowledge and general attitude*
- *the controller's reputation or the relationship of trust between the controller and the data subject*
- *the design of the choice architecture, including the communicated data protection risks caused by the concrete processing of personal data by the controller for the respective purpose.*

Data controllers and data subjects therefore have an interest in ensuring that the data subject can adapt the pre-settings of the automated system to the specific context of the service being used via a visual interface provided for this purpose.

However, to ensure that this interface design does not lead to the 'consent fatigue' caused by current cookie banners, it must disappear automatically after a reasonable period of time without the data subjects having to click it away. The reasonableness of this timeframe must be demonstrated by the provider through appropriate empirical tests (see below for further details).

(b) if the data subject uses the service again automatically and

(i) the data subject gave their consent or did not object during their previous visit, the controller shall not make a new request for consent or objection for the same purpose for the period during which the controller can lawfully rely on the respective legal basis; however, if the controller changes the data processing operation(s) to which the data subject has consented or has not objected, with the result that the data protection risks have increased since then, the controller must notify the data subject of this the next time they use the service, so that they can reconsider their decision;

(ii) if the data subject declined a request for consent, withdrew consent or objected during their previous visit, the controller shall not make a new request for the same purpose for a period of at least six months; however, if the controller changes the data processing operation(s) to which the data subject did not consent, did withdraw their consent or objected, with the result that the data protection risks have decreased since then, the controller may make a renewed request to the data subject the next time they use the service, so that they may reconsider their decision.

(iii) if the controller must or may make a further request according to previous points (i) and (ii), the design of the button or equivalent means used to adjust the choices must disappear automatically after a reasonable period of time.

Clarification:

Requirements (i) and (ii) ensure that data subjects are informed of changes relevant to their decision-making, even when using a service repeatedly, so that they can reconsider and adjust their previous decision. This rule applies not only to consent but also to objections, as the data subject has an equal interest in being informed and a need to make adjustments in both cases. To avoid click fatigue, the visual interface provided for this purpose must also disappear automatically after a reasonable period of time (iii) (see the visual examples given in the introduction).

Reason:

In line with the general technical developments, a service provider typically modifies the technical and organisational measures it employs to process data for a specific purpose. For example, it may select a new third-party provider or reconfigure an existing one, with the result that personal data may now be stored either within or outside the EU. These changes often lead to higher or lower data protection risks and are therefore – according to empirical studies – relevant to decision-making. Data subjects must be notified of such changes so that they can reconsider and adjust their previous decision.

For service providers, these ongoing notification obligations / opportunities represent a positive incentive to use (increasingly) data protection-friendly tools.

(c) notwithstanding previous points (a) and (b), the controller may make a further request to process the data subject's data if the data subject explicitly requested an additional service, feature or content ('contextual request') and has not indicated an affirmative decision by automated means.

Clarification:

The service provider's obligation to display a self-closing handover notice instead of the sticky cookie banner when the data subject uses automated and machine-readable means does not apply to so-called contextual consent (or other contextualised choice options).

Reason:

The problem of consent fatigue arises particularly when users first start using a service. This is because, at that stage, users primarily want to use the service rather than read the legal 'small print' in a tiny pop-up window. However, as soon as data subjects interact with specific content or functions of a service, the request to use their personal data for this purpose can be integrated into their user experience in a more intuitive way.

A classic example of this is consent to unlock additional services, such as a map, a video or social media content. If the data subject has not given their consent before, they can still do so later in the specific context of using that map, video or social media content (see the visual examples given in the introduction).

The advantage of such contextualised requests for data subjects is not only that they can be integrated more seamlessly into the context of use, but also that they are better able to understand the benefits and risks associated with disclosing their data for this purpose.

The seamless integration presupposes that it is tailored to the needs of data subjects. This must be demonstrated through empirical testing (see the reference to Article 25 GDPR in paragraph 7).

(3) Paragraph 1 (d) and 2 (b) (ii) shall not apply to controllers that

(a) are media service providers in the meaning of Art. 1(1)(d) European Media Freedom Act when providing a media service,

- (b) apply a legally compliant ‘pay-or-okay’ model to the processing of personal data for advertising purposes and
- (c) the data subject has not given their consent to the processing of their personal data for advertising purposes through automated and machine-readable means.

Where a controller processes personal data of a data subject for the purpose of personalised content, especially advertising, the controller shall ensure that their online interfaces on which the relevant advertising is displayed enable data subjects to exercise, via a technical-visual interface, their data subject rights according to Articles 15 et seq., especially their right to access and rectify their content, especially advertising, profile used for the display of the relevant content, especially advertising vis-à-vis the AdTech companies involved.

Clarification:

The provision ensures that the ‘pay-or-okay’ cookie banner, which media providers use to safeguard their business model, also functions with respect to automated and machine-readable means used by data subjects. To this end, the proposed wording includes a number of clarifications:

- *In particular, data subjects shall be able to communicate their consent to a ‘pay-or-okay’ cookie banner via automated and machine-readable means (see b). This significantly improves the user experience for a consenting data subject; at the same time, there is no reason for media providers not to receive a data subject’s consent via their automated and machine-readable means (see c). The obligation to accept signals of consent pursuant to paragraphs 1 (c) and 2 (a) and (b) (i) therefore do apply to them.*

To the contrary, if data subjects decline to give their consent via their automated and machine-readable means, media providers may present these data subjects with the alternative of paying for access to the media content when they want using the media service. Therefore, the obligation to accept signals of declined consent pursuant to paragraphs 1 (d) and 2 (a) and (b) (ii) do not apply to them.

- *The proposal also makes it clear that this exception applies only to data processing for the advertising purposes; the exception does not apply to other purposes, such as improving the media service, integrating third-party content or personalising the media service, as these purposes do not directly affect the business model of media providers and therefore do not justify preferential treatment over all other service providers.*

- *The remaining provisions – with the exception of paragraph 1(d) and paragraph 2(b)(ii) – also apply equally to media providers, as they improve the user experience (paragraph 1(a) and (b)) and significantly increase legal certainty (paragraph 1(e)) for data subjects, whilst at the same time not placing media providers at a disadvantage (see, in particular, paragraph 2(3)).*
- *Last but not least, the explicit reference to the legal definition of a media provider in Article 1(1)(d) European Media Freedom Act clarifies that the exception does not apply to other service providers that do not produce their own media content and/or take editorial responsibility for it, such as platforms pursuant to Article 3(i) DSA.*

*The legal privileges granted to advertising-financed business models of media providers go hand in hand with legal safeguards ensuring that processing of personal data for personalised advertising **as well as other personalised content** is carried out in a manner that complies with data protection legislation.*

Reason:

In respect of data protection compliant personalised advertising, a main challenge lies in ensuring transparency and intervenability on behalf of data subjects. The proposal therefore ensures that, in the immediate context of the advertisement displayed, the data subject can view and correct their advertising profile on which the advertisement is based.

To this end, media providers must only provide the visual interface as well as the personal data immediately available to them. The interface can then be used to make further personal data available via the ad tech companies, which are also involved in the delivery of the specific advertisements and, for their part, have direct access to personal data used for the advertisement.¹³

*This transparency prevents ‘creepy moments’ for the data subject, reduces their risk of manipulation and significantly boosts trust in personalised advertising **and other content**. Furthermore, the ability of data subjects to further tailor their advertising **/content preference** profile to their actual interests improves data quality and thus the effectiveness*

¹³ See the single interface recommended in European Commission, Directorate-General for Communications Networks, Content and Technology (DG CONNECT), Towards a More Transparent, Balanced and Sustainable Digital Advertising Ecosystem: Study on the Impact of Recent Developments in Digital Advertising on Privacy, Publishers and Advertisers, Publications Office of the European Union, Luxembourg 2023, ISBN 978-92-76-61811-9, DOI: 10.2759/294673., pp. 261 et seq.; see the research and development project ‘Secure in Data Traffic’ (SiD), funded by the German Federal Ministry of Research and Technology (BMFTR), in which the consortium partners – including the German Digital Economy Association (BVDW) – are developing a demonstrator for such a single interface. As the solution is currently only available as a research demonstrator, the proposed wording set out here does not contain any further requirements beyond the provision of the visual part of the single interface itself and the data immediately available; the further parts of such a single interface therefore continue to be governed by the general provisions of the GDPR, in particular Article 25.

of the advertisements or other content displayed.

The technical and organisational specifications are set out in a separate standard (see paragraph 7).

~~(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.~~

~~Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.~~

~~(5) Paragraphs 1 to 3 and 2 shall apply from [OP: please insert the date = 624 months following the date of entry into force of this Regulation].~~

Clarification:

For the sake of consistency, the provision on standardisation has been moved further down the list, as it applies equally to service providers and to browser and operating system providers. The former paragraph 5 on the temporal application therefore becomes paragraph 4.

The regulation on the temporal application now also applies to paragraph 3, as this contains not only an exception for media providers but also a requirement (see the provision in the 2nd sentence in section 3).

The deadline is being reduced from 24 months to 6 months.

Reason:

The shortened deadline is justified because, on the one hand, the technical systems for the automated and machine-readable indications of data subjects' choices are available on the market, and numerous relevant and tried-and-tested specifications and standards are in place, upon which standardisation in accordance with paragraph 7 can be based.

On the other hand, there is an urgent need on the part of data subjects, as well as data protection-friendly controllers and third-party technology providers, to finally enable informed decisions and, consequently, fair competition within the scope of data protection

law.

(56) Providers of web browsers, ~~which are not SMEs, and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment~~ shall provide the technical and visual interfaces means to allow data subjects to give their consent and to decline a request for consent, to explicitly request or decline an additional service, feature or content, withdraw consent or an explicitly requested service, feature or content and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means ~~referred to in paragraph 1 of this Article,~~ as applied pursuant to paragraphs 2 and 3 of this Article.

Clarification:

The wording makes it clear that browsers and operating systems must, first and foremost, provide the technical and visual interfaces through which automated and machine-readable means, by which data subjects indicate their choices, can communicate with the service used by the data subject (see the technical specification navigator.consent).

The wording of this section leaves open the question of whether providers of browsers and operating systems must additionally provide their own automated and machine-readable means available (however, see more details in the following sections).

The wording also extends the scope to include providers of operating systems. While browsers enable data subjects to communicate with websites, operating systems enable communication with applications.

Reason:

It is only through these technical and visual interfaces that data subjects can use their automated and machine-readable means to communicate with the websites they visit or the services they use.

Some browsers already enable this type of communication by providing technical and visual interfaces for so-called browser extensions. However, this does not apply to all browsers. For example, Google's Chrome browser for Android operating systems does not offer such an interface, meaning that the integration of automated and machine-readable means is still not possible.

As the problem of uninformed decisions arises not only when visiting websites but also when using applications, providers of operating systems must also make available the

interfaces that enable the integration of automated and machine-readable means.

This obligation also applies where data subjects use or want to use third-parties providing the automated and machine-readable means. The design of the integration of the automated and machine-readable means, be they from a third-party or not, must enable data subjects to make their choices in a simple and understandable manner, with a single-click button or by similar means. Browsers or operating systems are not required to integrate third-party providers of automated means if they are SMEs.

Clarification:

This provision makes it clear that the use of automated and machine-readable means must be as straightforward as possible for data subjects.

Providers of browsers and operating systems that do not reach a certain size are exempt from this obligation.

Reason:

Different browsers and operating systems have varying requirements (if they support the integration of automated and machine-readable means at all). Since, in practice, the likelihood of data subjects using these digital tools depends on how easy it is for them to use them, the provision ensures that their integration is as easy as possible for data subjects.

Providers of browsers and operating systems that do not reach a certain size are exempt from this obligation, in order to take their resources into account.

If the aforementioned providers of web browsers or operating systems are gatekeepers within the meaning of the Digital Market Act, they may not offer their own means for the automatic management of consents and objections.

Clarification:

The provision precludes browser and operating system providers from making their own tools available to data subjects if they are gatekeepers within the meaning of the Digital

Markets Act.

Reason:

Control over the design of automated and machine-readable systems confers a powerful position over a significant part of the data value chain on the internet. The specific design of decision-making architectures has a significant influence on how many data subjects consent to or object to the processing of their data, and thus on how much data can be processed for a wide variety of purposes.

When it comes to gatekeepers, the aim is therefore to prevent them from becoming even more powerful through their control of these decision-making structures.

To make matters worse, there is substantial evidence that gatekeepers (would) abuse this power to the detriment of their competitors. For instance, with ATT, Apple has designed the decision-making architectures in a way that has led to a significant reduction in consent rates for app providers on the Apple Store (whilst designing the choice architectures differently for its own advertising purposes and developing its own advertising business accordingly on this basis).

Until recently, Alphabet's plan was also to provide Chrome browser users themselves with the automatic and machine-readable means by which its users could have made their privacy choices for the websites they visited. It was only under considerable pressure from the competition authorities that Alphabet abandoned this plan.

Thus, if gatekeepers were allowed to provide the automated and machine-readable means themselves, it would be like putting the fox in charge of the henhouse.

(67) Paragraph 56 shall apply from [OP: please insert the date = 648 months following the date of entry into force of this Regulation].

Clarification:

The deadline is being reduced from 24 months to 6 months.

Reason:

The shortened deadline is justified because, on the one hand, the technical systems for the automated and machine-readable indications of data subjects' choices are available on the market, and numerous relevant and tried-and-tested specifications and standards are in

place, upon which standardisation in accordance with paragraph 7 can be based.

On the other hand, there is an urgent need on the part of data subjects, as well as data protection-friendly controllers and third-party technology providers, to finally enable informed decisions and, consequently, fair competition within the scope of data protection law.

(7) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, draft itself or request one or more European standardisation organisations to draft standards specifying the technical (including visual), organisational and legal requirements for the automated management of consents and objections. The standards shall:

- (a) ensure that the services of the various providers, in particular web browsers, operating systems, consent management platforms and services providing the automated and machine-readable means, are compatible and enable the seamless communication of data subjects' choices between them;
- (b) cover online and digital use, shall be technology-neutral and allow the aforementioned stakeholders the necessary scope to continuously improve the state of the art in accordance with Articles 25 and 23 GDPR.

~~for the interpretation of machine-readable indications of data subjects' choices.~~

Clarification:

*This wording sets out the specific requirements for the standard to be drawn up. **Of particular importance here is the explicit reference to Article 25 GDPR. The 'data protection by design' approach set out therein requires the controller to implement the requirements for informed consent and similar privacy choices 'effectively', taking into account the state of the art – that is, the scientifically proven most effective implementation currently available on the market.***

In its Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, the European Data Protection Board has already stated that demonstrating effectiveness is at the heart of the data protection by design approach (cip. 13 et seq.). Controllers must demonstrate effectiveness using appropriately suitable methods, whether of a qualitative or quantitative nature.

Demonstrating effectiveness is also crucial to the success and fair design of agent-supported choice processes. It ensures that these choice processes are not designed

in such a way that end users can either consent to the processing of their data as easily as possible or refuse it as easily as possible. Instead, these choice processes must be designed solely to enable users to make the most informed decision possible and thus to exercise the most effective control over the respective processing risks.

This is the only way to ensure that the legislative objective and the legal policy intention of fair competition are achieved.

Reason:

If the Commission possesses the necessary expertise, it should also be permitted to develop and publish a corresponding standard itself. This option also serves as a fallback arrangement, enabling the Commission to take charge of standardisation should the process organised by standardisation bodies drag on for too long.

In particular, the requirements regarding technological neutrality and the scope for further developing the state of the art, as set out in Articles 25 and 32 GDPR, are highly relevant in practice for ensuring the ongoing improvement of the automated and machine-readable means in line with general, continuous technological developments.

One negative example is the so-called Cookie Pledge Initiative, whose design requirements—some of which were very specific—were based on outdated knowledge and threatened to lock that outdated state of the art in place for years to come, thereby stifling any future improvements.

A positive example for standardisation is the proposal ConStand proposal that builds on various existing specifications and standards relevant in this field; it can be viewed here:¹⁴

https://cdn.prod.website-files.com/69b7b9ab93cf73e76cc11d89/6a0dc7dcb38e47e732616ddb_ConStand.pdf

The specifications and standards taken into account in ConStand include, amongst others:

- *Advanced Data Protection Control (ADPC),*
- *Global Privacy Control (GPC),*
- *ISO/IEC TS 27560 Consent Records and Receipts,*
- *W3C Data Privacy Vocabulary (DPV),*
- *Transparency and Consent Framework (TCF),*
- *Transparency Information Language and Toolkit (TILT),*
- *Yet Another Privacy Preference Language (YaPPL).*

¹⁴ See the introductory video at <https://consenter.euvideocdn.com/videos/6a0c5e191aa8709e21244663/3/video.m3u8>.

Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1 to 3 and 5.

Clarification:

The scope of the presumption of conformity rule has been aligned with all regulations setting out requirements for the various stakeholders.

(8) The competent authorities monitor and enforce the application of Articles 88 a and b as well as of the standards to be set up according to paragraph 7; the powers set out in Article 58 apply. In the event of an infringement of the provisions of Article 88(a) and (b), Article 83(1)–(3) and (5)–(9) apply. In order to be included in the European Data Protection Board’s list in accordance with sect. 1 lit. a sent. 2, providers of automated means must submit a corresponding application to the European Data Protection Board; the Board shall include the service in question in the list if the service complies with all the relevant requirements set out in sentence 1.

Clarification:

The provision makes it clear that the competent data protection authorities must also ensure compliance with the technical (including visual), organisational and legal specifications of the standards set out in paragraph 7.

For reasons of proximity to the subject matter, responsibility for conformity assessment lies with the European Data Protection Board as soon as a provider of an automated means submits an application for inclusion on the list within the meaning of Section 1(a).

Research background and institutions

The proposed wording for Article 88a and b Digital Omnibus set out here is the result of an interdisciplinary research process spanning more than 10 years involving various research institutes, in particular the Einstein Center Digital Future, the Alexander von Humboldt Institute for Internet and Society, the Berlin University of the Arts, and the academic spin-off Law & Innovation.

The academic spin-off [Law & Innovation](#) was founded to further develop the results of methodological basic research at the aforementioned research institutes into fully functional research demonstrators. The [Consenter](#) research demonstrator was developed to investigate and demonstrate the conditions for truly informed data protection choices and fair competition. Last October, the demonstrator was officially recognised by the German Federal Data Protection Officer as the world's first state-approved consent management service and publicly registered ([see the registry here](#)).

The [Einstein Center Digital Future](#) (ECDF) is Berlin's center for digitalization research. The ECDF stands for independent, interdisciplinary research on shaping and reflecting on digital transformation—together with businesses, policymakers, and civil society. Since its opening in 2017, the ECDF has been based on a unique public-private partnership model with more than 30 companies and organizations, as well as all four Berlin universities, Charité – Universitätsmedizin Berlin, and numerous other research institutions. Funded with €46.5 million by the Einstein Foundation Berlin, the ECDF is one of the most important initiatives for digitalization research in Germany.

The [Alexander von Humboldt Institute for Internet and Society](#) (HIIG) was founded in 2011 to research the development of the internet from a societal perspective and better understand the digitalisation of all spheres of life. As the first institute in Germany with a focus on internet and society, HIIG has established an understanding that centres on the deep interconnectedness of digital innovations and societal processes. The development of technology reflects norms, values and networks of interests, and conversely, technologies, once established, influence social values.

The [Berlin University of the Arts](#) (UdK Berlin) is one of the largest and most diverse art universities in Europe, where artistic teaching and practice intersect with academic discourse to shape its distinctive profile. With a history spanning more than 300 years, it is deeply rooted in the city of Berlin and, with more than 700 events each year, serves as a significant cultural driving force. UdK Berlin unites a broad spectrum of study programmes in Fine Arts, Design, Music, Performing Arts, and the academic disciplines related to these fields. Its profile is complemented by the Inter-University Centre for Dance Berlin and the Jazz Institute Berlin. For its approximately 4,500 students – about one third of whom come from abroad – the university offers excellent opportunities for study and research, fostering ongoing exchange between artistic practice and scholarly reflection.

Annex 1: Additional sales channel for publishers

Why is the European media industry lobbying against Article 88b of the Digital Omnibus—even though it is allowed to keep its "Pay or Okay" banners?

This is one of the most puzzling aspects of the current legislative debate.

Importantly, media service providers are exempt from the obligation to accept consent-agent signals. They may continue to display their existing "Pay or Okay" banners, allowing users to choose between personalised advertising and a paid subscription (see 1st picture below 👉). Given the economic importance of editorial media, this exemption is understandable from both a legal and policy perspective.

Article 88b requires service providers to respect users' privacy choices when these are communicated through trusted consent agents. Instead of responding to countless cookie banners, users could manage their preferences once and let their consent agent communicate them automatically. If designed properly, consent agents are the only known way in research and practice to ensure truly informed choices and, on this basis, fair competition for privacy friendly services.

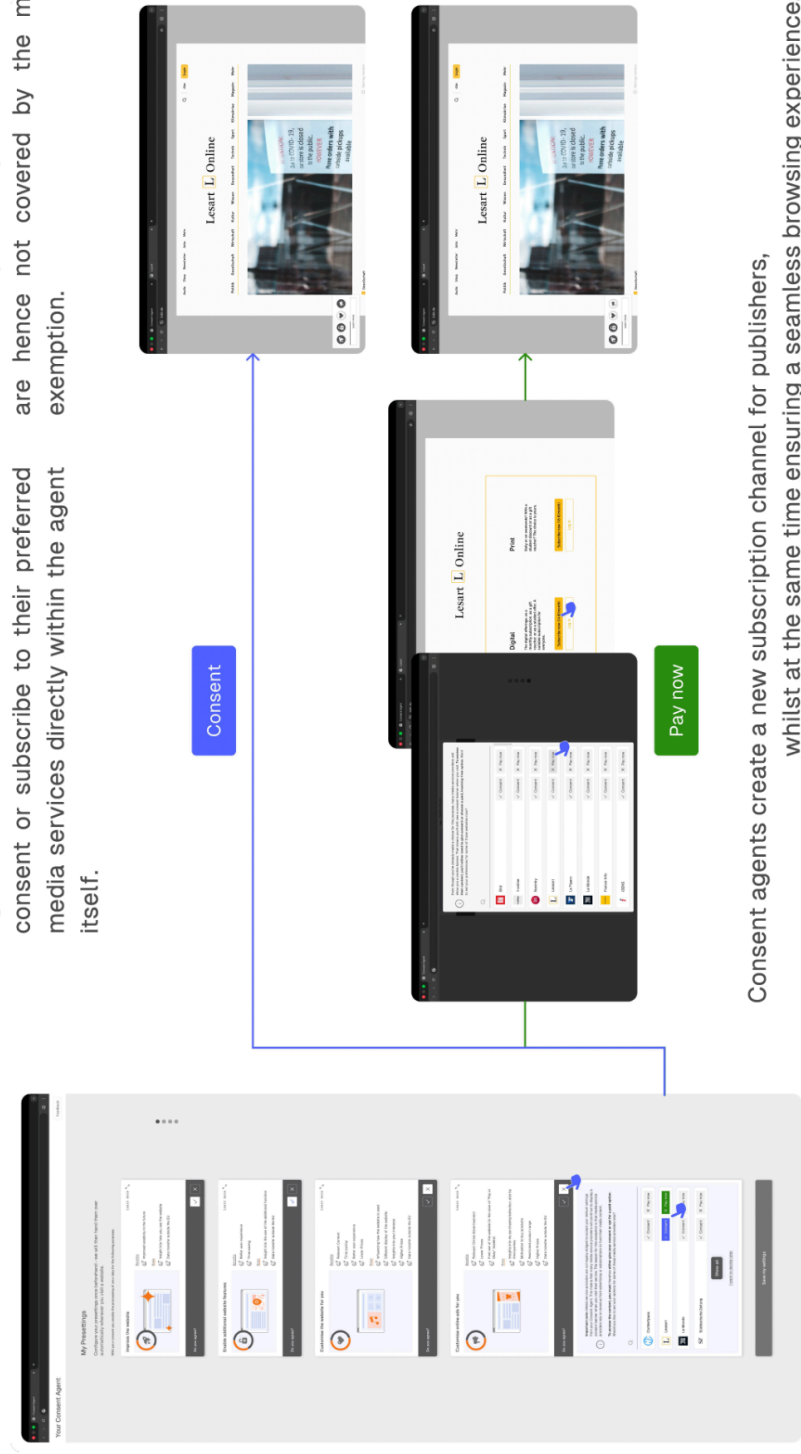


Article 88b does not weaken the media sector – it could strengthen it...

... if the media industry were to focus on the benefits of fair consent agents, rather than worrying about what it might lose if consent agents are unfairly designed (see Apple's ATT).

Well designed consent agents make their users aware of the fact that media services will need them to pay or consent to fund their content. To ensure a seamless experience, the consent agents will enable their users to either consent or subscribe to their preferred media services directly within the agent itself.

At the same time, Article 88b strengthens their competitive position vis-à-vis large platforms, which skim off a large portion of the financial value of their media content without bearing any editorial responsibility for it. Platforms are hence not covered by the media exemption.



Consent agents create a new subscription channel for publishers, whilst at the same time ensuring a seamless browsing experience.

Annex 2: Solving the issue with Apple’s ATT

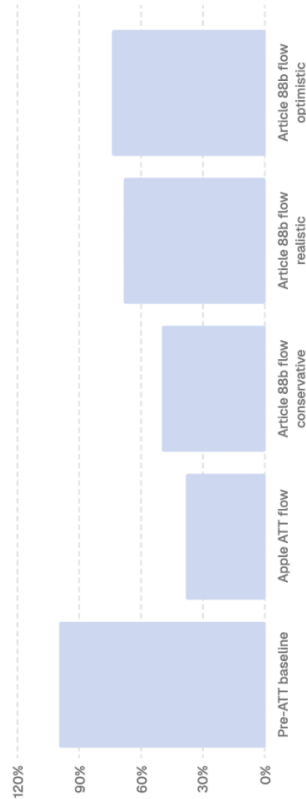
How can Article 88b Digital Omnibus address one of the biggest problems created by Apple's App Tracking Transparency (ATT)? Just compare the two click flows.

The following heuristic model calculation illustrates the potential positive effects of Article 88b Digital Omnibus for iOS/macOS app providers. The chart uses Apple's App Tracking Transparency Framework (ATT) as the starting point, mirroring the approach taken in Google's commissioned Implement study Gone in One Click.

ATT has reduced effective tracking rates substantially by complicating the consent flow and making consent to tracking unattractive for app users. Based on UX and conversion heuristics, simplifying the complicated consent flows through Article 88b could increase valid tracking consents by around 30–50% in a conservative scenario and by 70–100% in a realistic scenario. In many cases, this would nearly double the inventory available for personalised ads and marketing analytics.

Consent friction: ATT vs. Article 88b flow

Illustrative comparison using the ATT reduction cited by Implement/Google as the baseline and modelling the Article 88b flow as removing the additional ATT friction.



ATT: 60–65% relative drop in tracking rate cited by Implement/Google based on Kraft et al. (2023). Article 88b: heuristic scenario range, not empirical measurement.

Importantly, Article 88b would not restore the pre-ATT world. Some users genuinely do not want cross-app tracking and would continue to withhold consent. The purpose of Article 88b is thus not to increase consent rates by weakening privacy protections, but by simplifying consent flows and increasing the users' understanding of their benefits and risks of (different forms of) tracking.

In other words: whilst ATT offers its users more transparency and control, it unnecessarily complicates the consent process and makes tracking seem unattractive, regardless of the specific benefits and risks that the app entails. For users, however, it is the specific benefits and risks that are decisive, as these form the basis on which they decide whether or not to consent to the processing.

Article 88b would ensure that users make truly informed decisions by simplifying the consent process and clarifying the information that must be provided during the decision-making process. This, of course, requires the relevant wording to be included in Article 88b.

The example of ATT illustrates how decision-making processes should not be designed – and that Article 88b is about enabling users to make truly informed decisions, rather than nudging them, through repeated clicking actions, to either agree or refuse without understanding what this means for them in each case.

How does Article 88b improve the consent process?

The first graphic below shows the current situation under ATT. Users are often asked to give consent twice:

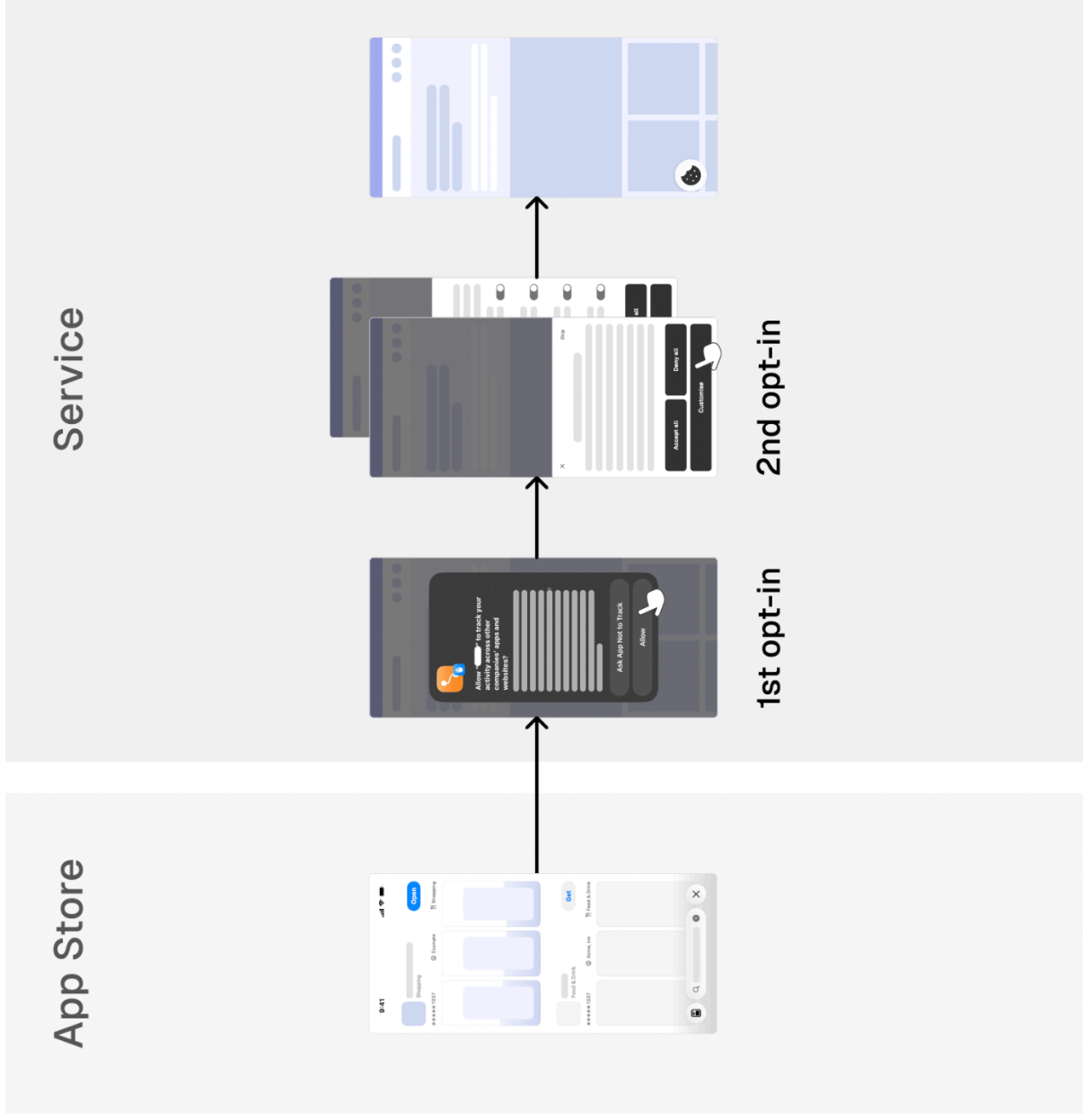
1. Consent to Apple's ATT (sharing its ad Identifier (IDFA) / cross-app tracking)
2. Consent to the app provider's specific processing purposes (e.g. personalised advertising, marketing analytics)

Every click creates friction for end users. ATT's design is also regarded as discouraging users from sharing the IDFA. The result: lower consent rates and financial losses for app providers.

The second graphic shows how Article 88b can improve this process: Instead of asking users repeatedly, preferences are set once through a consent agent and then communicated to services through machine-readable signals.

In the process, users are informed in increasing detail about the specific level of data protection offered by the service. Users remain fully in control and can adjust their preferences at any time, but unnecessary click friction disappears.

Current situation:
Apple's ATT
without Art. 88b
Digital Omnibus



Every single app
requires the
following fatiguing
double opt-in

