A design and methodology toolkit for developing and validating effective consent and other decision-making mechanisms

1. Introduction

This design and methodology toolkit is intended to aid the development and validation of effective consent and other decision-making mechanisms. It summarises the findings from more than a decade of interdisciplinary research at the intersection of data protection law, user experience and user interface design, human-computer interaction, behavioural economics and entrepreneurship research.[1]

According to this, there are three key factors that influence the effectiveness of informed consent:[2]

1. The prior knowledge and attitude of the individual internet user;
2. the fundamental trust that an internet user places in the website visited or the service used; and
3. the way in which a service informs its users about how it intends to process their data.

The design and methodology toolkit presented here focuses on the third point.

Service providers that process personal data, such as website operators, face a conflict of objectives when informing their users about the use of their data. On the one hand, they wish to build trust among their users in the use of their service, their brand and the disclosure of data. On the other hand, many services strive for the highest possible formal consent rate so that they can process as much data as possible.[3]

---

[1] See the research projects carried out by the Digital Self-Determination Research Unit at the Einstein Center Digital Future – Berlin University of the Arts (https://www.ziw.udk-berlin.de/nc/en/research/digital-self-determination/) and those within the research programme 'Data, Actors, Infrastructures: Governance of Data-Driven Innovation and Cybersecurity at the Alexander von Humboldt Institute for Internet and Society (https://www.hiig.de/en/research/data-actors-infrastructures/).

[2] See, for example, Dinev, Tamara/Hart, Paul, An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research 17 (2006), S. 61–80; Culnan, Mary J./Armstrong, Pamela K., Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science 10 (1999), S. 104–115; Pavlou, Paul A., Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, International Journal of Electronic Commerce 7 (2003), S. 101–134; McDonald, Aleecia M./Cranor, Lorrie Faith, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 4 (2008), S. 543–568; Nouwens, Midas et al., Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), 2020, S. 1–13; Schaub, Florian et al., Designing Effective Privacy Notices and Controls, IEEE Internet Computing 21 (2017), S. 70–77.

[3] See, for example, Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on Art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924.

When considering how services resolve this conflict of objectives, a distinction is often made between so-called ‘bright patterns’ or neutral techniques and ‘dark patterns’.[4] The term ‘dark patterns’ refers to a service using techniques that

1. leave its users in the dark about the specific presentation of the information regarding the risks associated with disclosing their data, thereby preventing them from making an informed decision about the benefits and risks of data disclosure, and/or

2. makes it difficult for its users, through the specific design of the decision-making architecture, to make a decision in line with their own assessment of the benefits and risks.

The following discussion focuses on neutral techniques, or ‘bright patterns’, which, through the appropriate design of the information and decision-making architecture, demonstrably enable informed decisions. Although irrelevant from a data protection perspective, it should be noted – given the business sector’s considerable interest in the matter – that a user-friendly implementation of informed decision-making processes can lead to an increase in consent rates.[5]

Since, in practice, the use of such techniques was (and still is) by no means a given, and dark patterns are frequently used instead for the collection of personal data, the legislator felt compelled to lay down legal requirements to facilitate effective decision-making processes. These legal requirements are briefly listed in the following chapter.

2. Legal requirements

Article 6(1)(a) GDPR requires informed consent as one of the possible legal bases for the processing of personal data. According to Article 4(11) of the GDPR, consent is

> *“any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*”.

Article 25 of the GDPR sets out further requirements for the implementation of informed consent. In particular, the controller – for example, a website operator – must implement informed consent in such a way, both technically and organisationally, that protection against the risks posed by data processing to the fundamental rights of data subjects is effective.

---

[4] Leiser, M. and Santos, C., Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface (April 27, 2023). Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface, Vol. 15 No. 1 (2024): BILETA Special Issue , Available at SSRN: https://ssrn.com/abstract=4431048; Bielova, N. Survey of academic studies measuring the effect of dark patterns on acceptance consent rate of users in consent banners; Graßl, P., Schraffenberger, H., Borgesius, F., and Buijzen, M., Dark and bright patterns in cookie consent requests.

[5] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894.

In this context, the **state of the art** must be taken into account, which means the most effective implementation of informed consent currently available on the market ("best available technology"). The state of the art represents a so-called dynamic reference to the current stage of development. Conceptually, the state of the art demands more than the so-called best practice rules, because it requires evidence that the implementation in question is indeed the most effective. On the other hand, the state of the art requires less than the so-called state of science, because it does not require the implementation of every concept that is scientifically proven to be the more effective one, but only one that is already available on the market. Beside the state of the art, the data controller may take the implementation costs into account. This means that the controller does not have to implement the state of the art if the costs involved are disproportionate.[6]

In line with this, the European Data Protection Board (EDPB) makes it clear in its Guidelines 4/2019 on Article 25 Data Protection by Design and by Default that demonstrating effectiveness is the central element of Article 25 of the GDPR. The EDPB states:

> *"To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective. KPIs may be quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.*"[7]

In practice, the **greatest challenge when implementing effective consent** currently lies in ensuring **informed** consent. To date, little evidence of effectiveness has been provided in practice. On the contrary, there are numerous empirical studies demonstrating that conventional cookie banners do not provide internet users with sufficient information.[8] According to these studies, whilst consumers do prefer data protection-friendly services over

---

[6] See at Hansen, M. in: Datenschutzrecht – DSGVO/BDSG, Simitis, S., Hornung, G. and Spiecker genannt Döhmann, I. (Eds.), Art. 25 cip. 36/37 and Art. 32 cip. 27 et seq.; see regarding the regulatory concept and its intended impact on market dynamics, Grafenstein, M. v. (2019). Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design, in: González-Fuster, G., van Brakel, R., & P. De Hert, Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed.. Cheltenham: Edward Elgar Publishing.

[7] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p. 7: "To this end, the controller may establish appropriate key performance indicators (KPIs) to demonstrate effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves its data protection objective. KPIs may be quantitative, such as the percentage of false positives or false negatives, a reduction in complaints, or a reduction in response time when data subjects exercise their rights; or qualitative, such as performance evaluations, the use of grading scales, or expert assessments. As an alternative to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards."

[8] 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.

those with higher risks, they are unable to recognise them and therefore cannot opt for them.[9]

At best, current practice involves the application of the aforementioned best practice rules. As said, these best practice rules differ from the state of the art in that the controller is not required to provide empirical proof of effectiveness. **However**, **best practice does not meet** the standard required by **Article 25 of the GDPR**, which demands proof of effectiveness.[10]

There are numerous academic and practical contributions on how consent processes should not be designed.[11] Even where positive guidelines are provided, these represent only best practice rules, but no empirical evidence that they enable effective decision-making processes. On the contrary, a quantitative study has shown that internet users click away from cookie banners designed in accordance with best practice rules in such an uninformed manner that one can hardly speak of 'informed' consent within the meaning of the law.[12]

Against this backdrop, the following chapters summarise the findings and methods from a research and development process that the author of these guidelines has undertaken over the last 10 years, and which can be used to **positively define and further develop the state of the art**.[13]

3. Design factors for developing effective decision-making mechanisms

Presenting information relevant to data protection law in a clear and accessible manner not only significantly contributes to internet users being better informed about the processing of their personal data, but also fosters greater trust in the use of the service and in the disclosure or processing of their data. A clear and accessible presentation therefore also has a significant influence on the likelihood of internet users consenting to or objecting to the disclosure of their data.[14] According to the current state of the art in the meaning of Article 25

---

[9] 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.

[10] Hansen, M. in: Data Protection Law – GDPR/BDSG, Simitis, S., Hornung, G. and Spiecker-Döhmann, I. (Eds.), Art. 25 para. 36/37 and Art. 32 para. 27 et seq.

[11] See, for example, CNIL, Bielova, N. (2023). A survey of user studies as evidence for dark patterns in consent banners, available at https://linc.cnil.fr/en/survey-user-studies-evidence-dark-patterns-consent-banners.

[12] 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; ibid (longer version including all pictures and charts), available under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5012997; siehe bereits Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centred UX-design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722.

[13] See footnote 1.

[14] See the White Paper Informed consent as a key to fair competition; in more detail Adjerid, I., Acquisti, A., Brandimarte, L., Loewenstein, G. Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, in: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS), 2013; Ebert, N., Pape, S., Spohr, D., Bingel, J. Bolder is Better: Raising User Awareness for Data Privacy through Visualisations. arXiv, 2021; Godinho de Matos, A., Godinho de Matos, M.,

and 32 GDPR, providers of websites and other digital services should focus on the following factors to enable effective decision-making processes. The following factors have not only been scientifically proven to be the most effective means of implementing informed consent, but are also available on the market.[15] The following account, of course, does not claim to be exhaustive or definitive. Instead, the state of the art of informed consent will (hopefully) continue to evolve.

3.1 Purpose specification regarding the benefits and risks of the data processing

From the user's perspective, the information most relevant to their decision-making is details regarding the purposes for which their data is processed, and the associated benefits and data protection risks.[16] The focus on the **purposes of processing** is consistent with the data protection legal framework, according to which the purposes of processing are the cornerstone of the data protection assessment. The presentation of the benefits and risks not only corresponds to the function of the principle of purpose limitation, according to which internet users must be able to assess the consequences for themselves on the basis of the specification of the purpose.[17] It also corresponds to behavioural economic theories of privacy calculus, according to which laypeople always weigh up the associated benefits and disadvantages when making decisions about disclosing their data.[18]

The clear **presentation of the benefits and risks** associated with the respective processing purpose **represents one of the two decisive turning points** in the evidence-based development of effective decision-making processes. Various qualitative and quantitative studies show that presenting the benefits and risks can significantly improve end-users' understanding. The greatest gains in understanding can be achieved in combination with agent-based decision-making processes (see point 3.1.3 below).[19]

Based on the current state of research and development, it is recommended that the following processing purposes be formulated (the additions in brackets merely refer to the legally required default settings):

Adjerid, I. Consumer Consent and Firm Targeting after GDPR: The Case of a Large Telecom Provider, Working Paper, 2022.

[15] See the Consenter research demonstrator, which has now been developed into a market-ready solution, available at www.consenter.eu.

[16] For further legally required information, see the relevant legal literature; for information relevant from a user's perspective, see, for example, Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on Art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924.

[17] Art. 29 Working Party, Opinion 03/2013 on purpose limitation, pp. 11 et seq.

[18] See Dinev, T., Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research 17, pp. 61–80, 61; fundamentally, see Culnan, M. J., Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science 10, pp. 104–115.

[19] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; see in greater detail Gerber, N., Grassl, P. and v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

1. Anonymous improvement of the service (opt-out)
2. Improvement of the service (opt-in)
3. Enabling additional website functions (opt-in)
4. Customisation of the website (opt-in)
5. Support for marketing analyses (opt-in)
6. Receive marketing offers (opt-in)
7. Receive personalised marketing offers (opt-in)
8. Personalisation of online advertising (opt-in)
    a. Profile-based personalisation
    b. Reminder advertising (= retargeting) → still under discussion
    c. Group-based personalisation
    d. Context-based advertising

This list of purposes is not exhaustive and does not claim to be exhaustive. Further processing purposes, which depend on a decision by the respective internet user (i.e. an opt-in or opt-out procedure), are just as possible as other, even clearer formulations if evidence is supporting this.

Specifying processing purposes, it is crucial for the wording that, on the one hand, it conveys to internet users a sufficiently concrete idea of why and how their data is processed. On the other hand, it must be specific enough to allow the concrete risks to fundamental rights posed by each processing operation to be identified and distinguished from other processing procedures.[20]

As the previous list shows, the purposes may stand in different relationships to one another. As examples 6 to 8 of the purposes show, hierarchies of purposes can be formed which are either mutually exclusive (examples 6 and 7) or complementary (examples 8(a) to (d)). Differently worded purposes that describe the same processing procedure and entail either the same or greater or lesser benefits and risks can be mapped using a translation matrix (see, for example, the purpose formulations in the Transparency and Consent Framework of IAB Europe).[21] Where applicable, these discrepancies must be disclosed to internet users (see section 3.1.3 for further details).

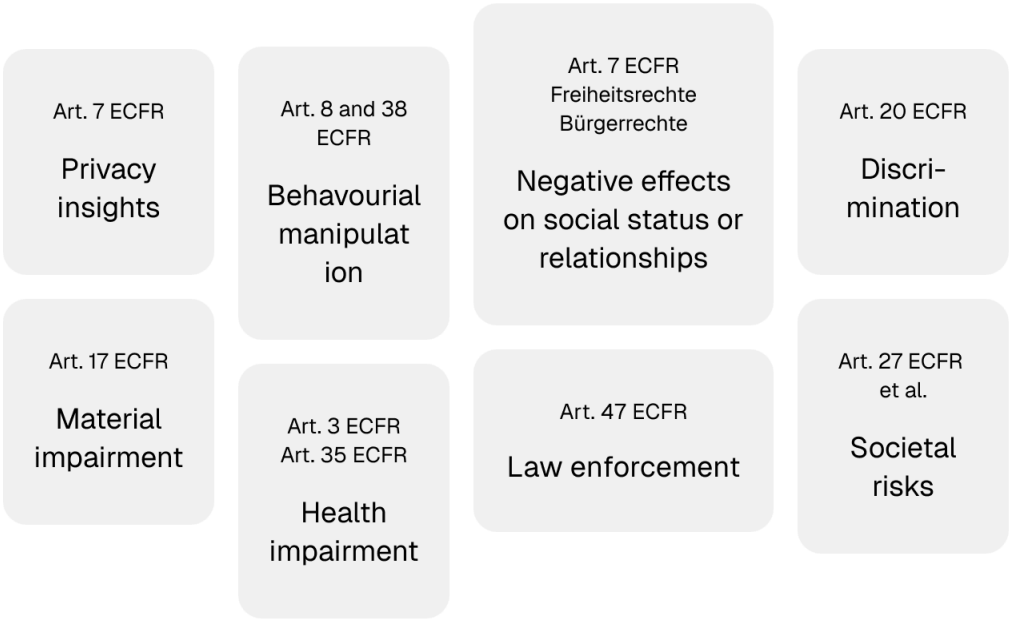
It can be assumed that purposes can be formulated in an even more comprehensible manner and that the state of the art will continue to evolve accordingly.

---

[20] Grafenstein, M. v. (2021). Refining the concept of the right to data protection in Article 8 ECFR – Part III. European Data Protection Law Review, 7(3), 373–387. DOI: 10.21552/edpl/2021/3/6 with further references.

[21] See also Annex 1 of the specification ConStand (in review).

The results of several legal and empirical research projects can be drawn upon to present the risks. According to these results, the risks relevant from the user's perspective largely correspond to the **risks to fundamental rights**:[22]



These risks must be assigned to the respective processing purpose and weighted on a scale of 1–3 (1 = low risk; 2 = medium risk; 3 = high risk). The assignment and weighting of risks must be carried out on the basis of established methodologies for determining data protection risks.[23]

When presenting the risks to internet users, the focus should be on the risks to the individual fundamental rights of the respective internet user that result directly from the processing purpose. The indirect, i.e. abstract, risk that the data might be misused is classified here as a risk to the security of processing in accordance with Article 32 of the GDPR. IT security risks pursuant to Article 32 of the GDPR, as well as societal risks, such as those to democracy or solidarity within a society, have not yet been represented in the research designs underlying the following visual examples. The reason for this is that, in previous iterations of the designs, this led to the test subjects being overwhelmed.[24]

---

[22] Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centred UX design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722, pp. 20/21.

[23] See, for example, the standard data protection model in its latest version, published at https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

[24] Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on Art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924; Gerber, N., Grassl, P. and v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

Therefore, there is considerable potential for further development in the state of the art here, to map not only concrete individual risks but also abstract (i.e. security) risks and societal risks without overwhelming users.

The benefits that internet users derive from disclosing their data for the specific purpose should also be identified and weighed against the respective processing risks. According to current knowledge, the allocation of risks and benefits has a significant influence on awareness, trust and, consequently, the consent rate.[25] The utmost care must therefore be taken in the allocation and weighting to ensure that no risk is presented as smaller or larger than it actually is. The same applies to the presentation of the benefits. The correct allocation and weighting should therefore ideally be validated through a multi-stakeholder process involving laypeople and experts active in various fields, particularly in data and consumer protection as well as in the various – competing – economic sectors (see also section 4.2).[26]

3.2 Layout and visual presentation / hierarchy

When it comes to visual presentation, there is usually a conflict of objectives: from a legal perspective, the information must be presented as precisely and comprehensively as possible. From a behavioural economics perspective, the information should be condensed to its essential content so that laypeople can absorb and understand it.[27] The following design principles can guide the resolution of this conflict of objectives:

Information that is crucial for internet users to make decisions should be supported by **visualisations and/or icons**. Initially, visualisations and icons cannot and should not replace textual explanations; over time, internet users can become familiar with them, so that they can eventually replace the textual presentation.[28]

As a general rule, **the fewer textual and visual elements there** are **on a given visual level, the more readily laypeople will perceive and understand the information**. This does, however, exacerbate the conflict of objectives described at the outset. This conflict of objectives can be resolved by distributing the information across different visual levels.[29] In

---

[25] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; siehe in größerem Detail Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

[26] Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on Art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924; Gerber, N., Grassl, P. and v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (under review).

[27] Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924 with further references.

[28] For details on the balancing decisions to be made regarding a textual and visual presentation that is as comprehensible as possible, see, for example, Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on Art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924 with further references.

[29] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, p. 19.

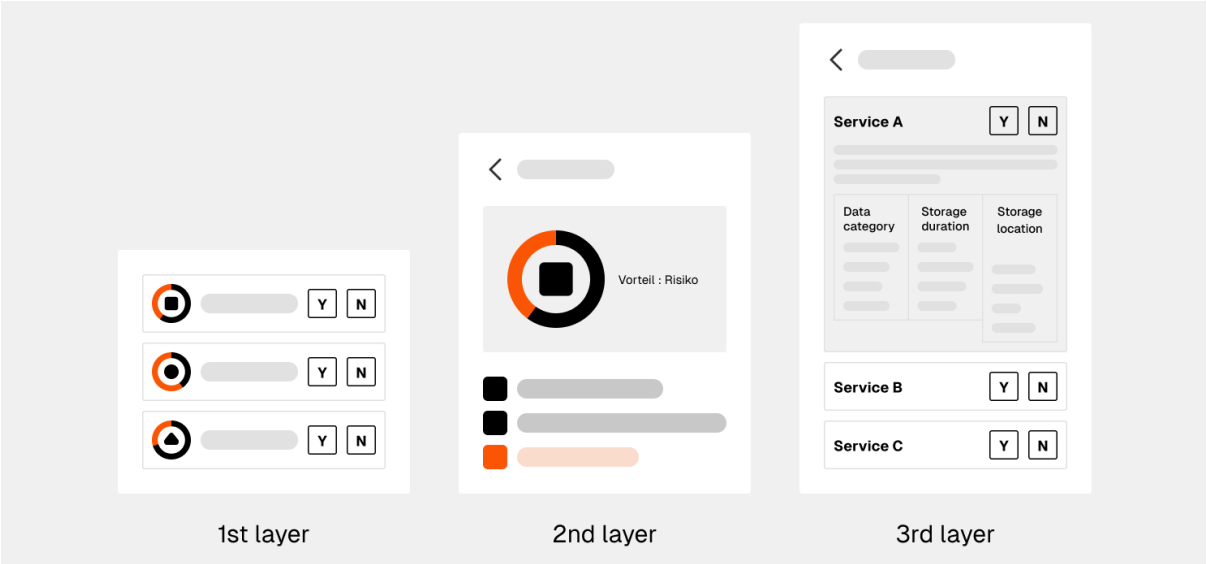
doing so, the following should be prioritised: the information most relevant from the user's perspective should be placed on the first visual level, whilst the less relevant information should be placed on the subsequent visual levels.

According to the current state of the art, **the purposes** should be displayed **on the first visual level** alongside the relevant privacy icon. In the research demonstrator Consenter referenced here, the respective benefits and risks are not yet depicted individually on the first visual level, but are instead condensed into a benefit-to-risk ratio. The **benefit-to-risk ratio** displayed is decisive for internet users and significantly influences the consent rate.[30]

Presenting all individual data protection risks and benefits for each purpose on the first level has so far proved challenging, as it involves a great deal of information at once, which has a negative impact on internet users' intuitive understanding. The **presentation of the individual risks and benefits** is therefore **only** shown **on the second visual level**. This also includes a list of risks that do not occur. This is intended to prevent internet users from 'imagining' risks that are actually not caused by the respective processing purpose.[31]

At the third level does a presentation follow detailing which data is collected, which **third-party providers, if any**, are granted access to this data, and for how long and where this data is processed. At subsequent layers, further information is presented, such as that the legislator considers relevant for informed consent.

When it comes to the question of which information must be presented at which visual level and in what manner to ensure that internet users are optimally informed, there is, of course, scope to further develop the state of the art.



[30] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; see in detail Gerber, N., Grassl, P. and v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (under review).

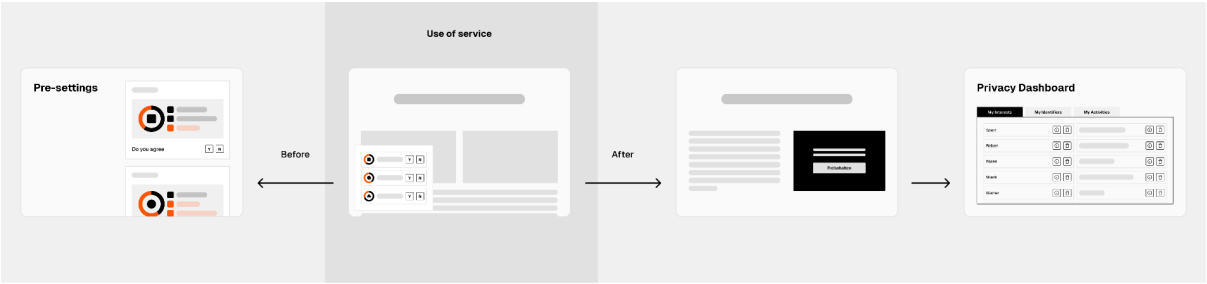
[31] See the increase in false negatives due to greater transparency in Gerber, N., Grassl, P. and v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (under review), as well as protection against "diffuse fear" in BVerfG, 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, and 1 BvR 586/08 (data retention), p. 241

3.3 Timing and context of the request

The second decisive turning point in the evidence-based development of effective decision-making processes is its proceduralisation. Internet users are best placed to understand the complex processing procedures in terms of the positive and negative consequences for their lives if they are given several sequential opportunities to do so at different points in time. These tiered information and decision-making architectures facilitate a learning process.[32]

According to current knowledge, in addition to the classic cookie banner, there are essentially two further so-called touchpoints[33] available, which precede the classic cookie banner on the one hand and follow it on the other:

- On the one hand, so-called consent agents, which bring information and decisions forward, i.e. make them possible before the respective service is used.
- Secondly, contextualised information and intervention options, through which internet users can receive information and/or exercise their data subject rights in the specific context of use (for example, by means of so-called contextual consent).



Consent agents, consent management services, Personal Information Management Services (PIMS)

Solutions that precede a traditional cookie banner enable internet users to inform themselves in advance at a central point about recurring data requests and to set appropriate default preferences. Such solutions offer internet users three main advantages:

1. Internet users can find out about data requests at a time *of their choosing*; this allows them to devote significantly more attention to the information.
2. Internet users can deal with recurring and therefore tiresome information in advance and, when visiting a website or using a service, concentrate on any deviations from the standardised information.

---

[32] See Prince, C., Omrani, N., Schiavone, F. Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. Information, Information Technology & People (2024) 37 (8): 1–24; Kumar, P.C. (2022). Toward a Practice-Based Approach to Privacy Literacy. In: Smits, M. (eds) Information for a Better World: Shaping the Global Future. iConference 2022. Lecture Notes in Computer Science(), vol 13192. Springer, Cham. https://doi.org/10.1007/978-3-030-96957-8_13.

[33] On the concept as a component of a broader user journey: Lemon, Katherine N. and Verhoef, P. C. (2016). Understanding Customer Experience Throughout the Customer Journey, in: Journal of Marketing, Vol. 80 (6), 2016, pp. 69–96; Hassenzahl, M., Experience Design: Technology for All the Right Reasons. San Rafael (Morgan & Claypool Publishers) 2010.

3. Internet users can also use default settings to set aside recurring and therefore tiresome requests to consent to or object to the use of their data. When visiting a website or using the relevant service, they can then adjust these default settings in light of the specific circumstances of the service.

   Here, the reputation of the service, the trust that internet users have in a service, and the specific level of data protection communicated become decisive factors. If the service enjoys a high reputation among internet users, or if they trust the processing of their data by the specific service – for example, because it convincingly communicates its above-average level of data protection – this can significantly increase the likelihood of consent.[34]

   It is important that internet users can make these adjustments, but are not obliged to do so. If internet users do not make any adjustments within a certain period, the button disappears automatically. This resolves the issue of so-called ‘consent fatigue’.[35]

Contextualised information and intervention options (e.g. contextualised consent)

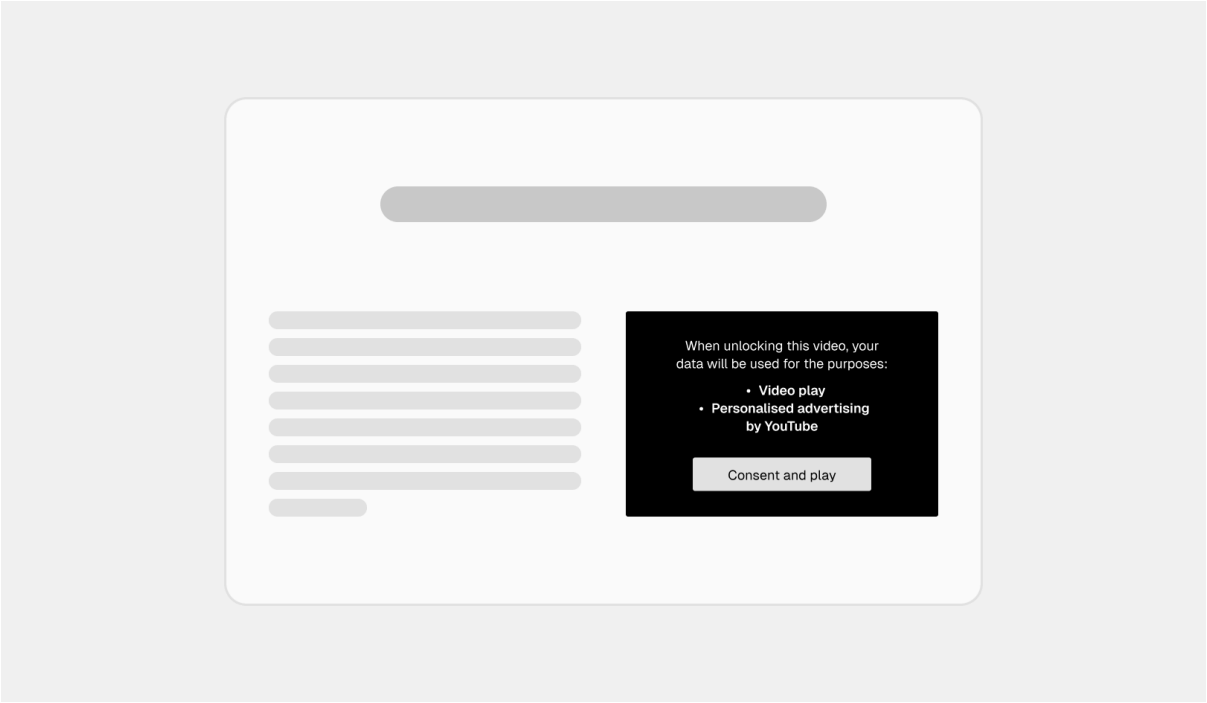
Solutions that follow on from a traditional cookie banner enable internet users to inform themselves about data processing and make appropriate decisions with regard to a specific function or piece of content on the website with which they are currently interacting. Such solutions offer the following key advantages for internet users:

- Through contextualisation within the respective usage context, internet users better understand the specific reason for data collection and, consequently, the extent of the processing and its consequences. For example, if personal data is required to play a video and users only unlock the video by giving their consent, the benefit of sharing the data becomes immediately clear to them at that very moment – unlike when simply visiting a website.

  If the provider also wishes to use the data for its own advertising purposes, this must be made clear. This allows users to understand which of their data is being used by

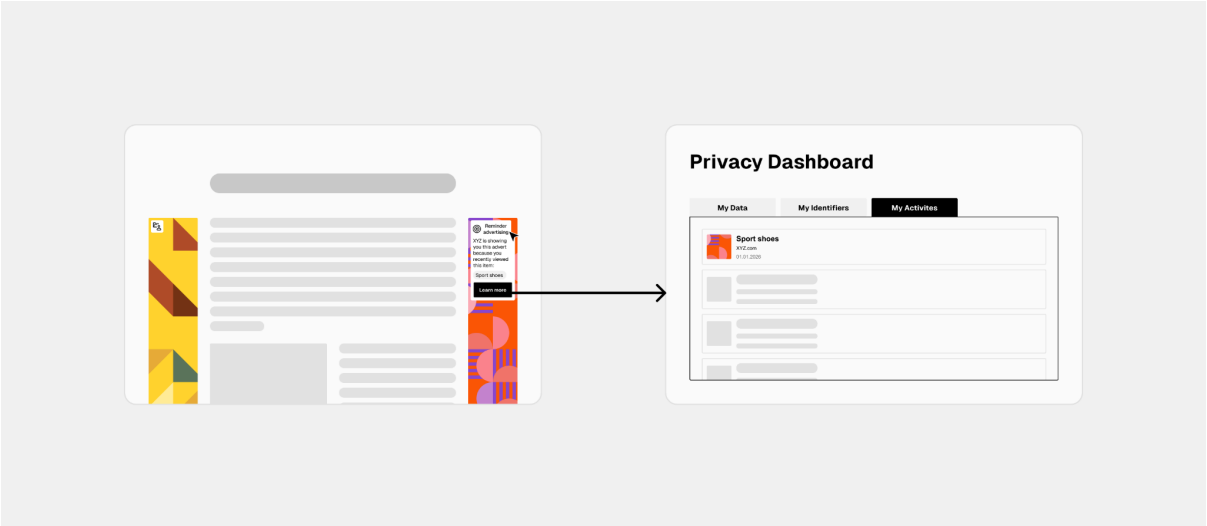
[34] Gerber, N., Grassl, P. and v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (under review).
[35] On the problem of consent fatigue with a focus on cookie banners Nouwens, Midas et al. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence, in: CHI Conference on Human Factors in Computing Systems (CHI 2020); with a focus on privacy policies McDonald, A. M., Cranor, L. F. (2008). The Cost of Reading Privacy Policies, in: I/S: A Journal of Law and Policy for the Information Society, Vol. 4 (3), 2008, pp. 543–568.

which provider for advertising and how this is done (see below). Website operators often fail to fulfil this obligation to highlight the additional processing purposes of the third-party service. Instead, there is often only a general reference to the privacy policy of the respective service. However, as this information is relevant to internet users when deciding whether or not to disclose their data, the operator of the website or service must directly highlight these additional purposes of the third-party provider. These connections become much clearer in the specific context of using the respective service.



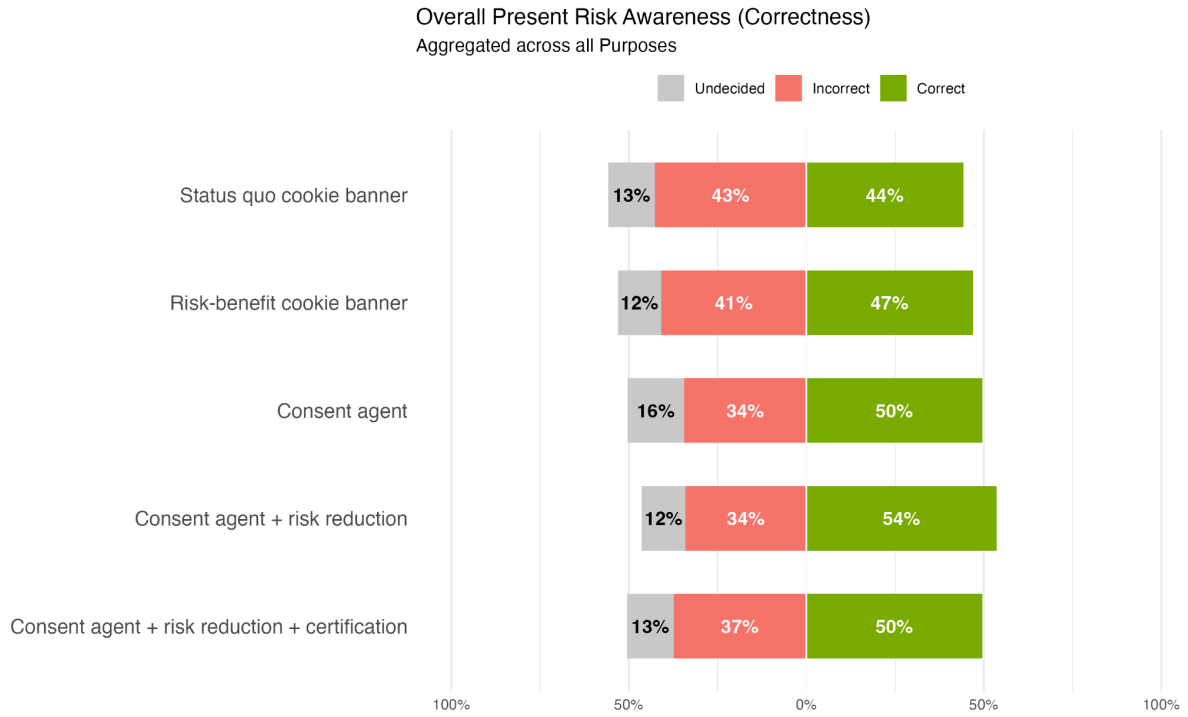
- Internet users also understand their other data subject rights better when these are explained in the specific context of use. These include, above all, the right to access, rectify and erase their data. If, for example, personalised advertising is displayed to them, it should be explained directly there and then on which personal data this advertising is based. In concrete terms, this means: it should be clear what interests the advertising industry attributes to them – and on what data these assumptions are based. This allows users to assess whether they consider this data processing to be appropriate, whether the assumed interests correspond to their actual interests, and whether they wish to correct or delete the underlying data.[36]

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



Side note: Informedness based on a quantitative A/B/n test

The combination of the various touchpoints for internet users forms a learning process that leads to them being significantly better informed. A quantitative A/B/n test conducted in 2024 revealed that, in particular, the integration of consent agents combined with opportunities for internet users to interact with the specific service – during which they receive further information on the service's specific data protection standards and can adjust their default settings – leads to a significantly higher level of awareness than previous banners.[37]



[37] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; For further details, see Gerber, N., Grassl, P. and v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (under review).

It should be noted that the designs underlying this study were still at a preliminary conceptual stage (see Annex 1). The same applies to the contextualised integration of other data subjects' rights, particularly in relation to personalised advertising or other personalised content, where there are as yet insufficient studies examining the impact of user-friendly implementations on awareness.[38]

There is still considerable scope here to further develop the state of the art and significantly increase awareness.

3.4 Granularity of choice options / design of the buttons

The combination of traditional cookie banners with consent agents also allows for further flexibility in the design of the choice buttons. According to current best practice guidelines, cookie banners are (mostly) designed as follows:[39]

- All processing purposes on which internet users can make a decision are listed on the first visual level.

  IMPORTANT: Unlike the approach advocated in the design guidelines of the Good Practice Initiative for Cookie Banner Consent Management, these purposes must therefore already be individually selectable on the first visual layer. Listing such purposes on a subsequent layer constitutes a dark pattern, as it makes granular decision-making more difficult for the internet users.

- Processing purposes that do not require a decision from internet users must not be displayed on the first visual level, as they distract internet users from the essential decision-making options.

- The first visual level must list not only processing purposes that require consent (opt-in), but also purposes to which internet users can object (opt-out).

  Important: Displaying such opt-out purposes on a subsequent layer constitutes a dark pattern, as it makes it more difficult for internet users to make a decision and is therefore less effective.

- Depending on legal requirements, the button for the respective processing purpose must be disabled by default (opt-in) or may be enabled (opt-out).

  IMPORTANT: A neutral default setting for the button constitutes a dark pattern as long as internet users cannot bring these decisions to the forefront by using a consent agent, because it requires additional clicks and thus exacerbates the problem of consent fatigue. This, too, is a point that is frequently overlooked in current best practice guidelines.

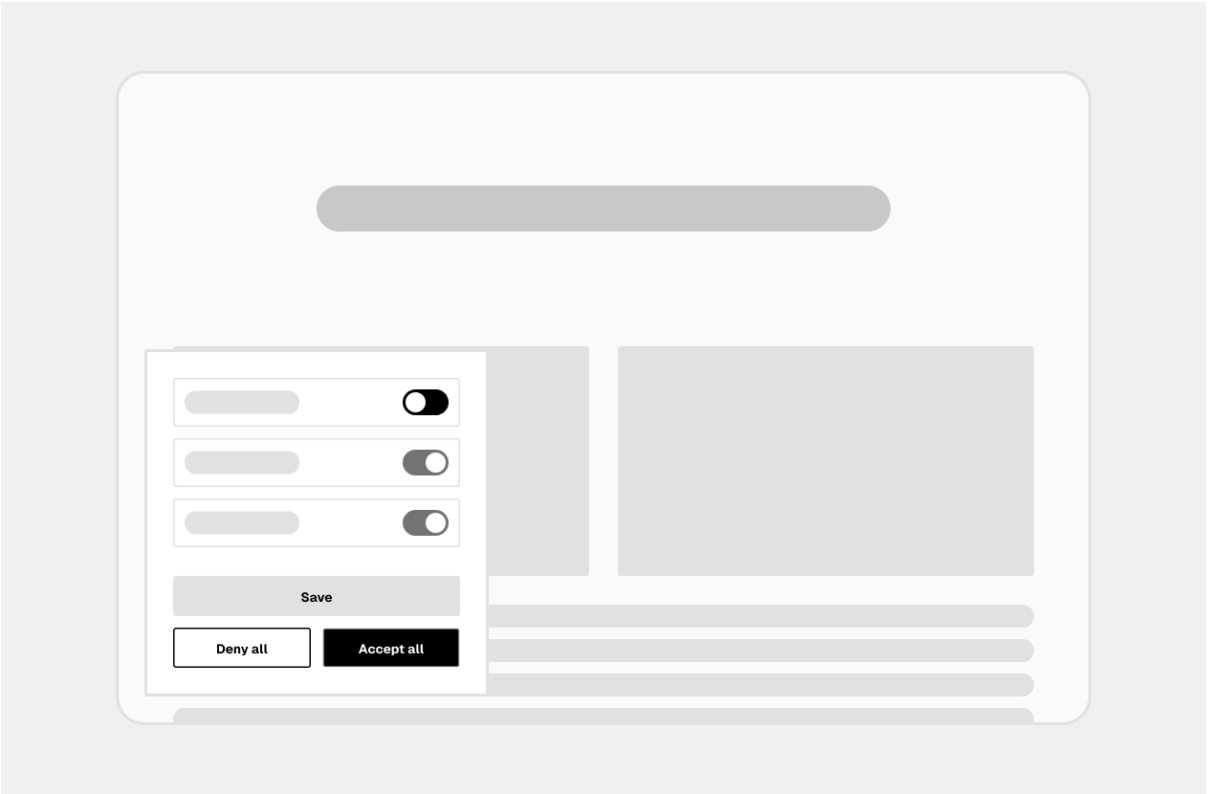
---

[38] Siehe hierzu aber das laufende Forschungsprojekt Sicher im Datenverkehr (SiD), online abrufbar unter https://sid-projekt.de/.

[39] See, apart from a few exceptions, the Good Practice Initiative for Cookie Banner Consent Management – Design Guidelines at https://hdr4.bmj.de/SharedDocs/Publikationen/EN/Cookie_guidelines.pdf?__blob=publicationFile&v=3&utm_source=chatgpt.com.

- In addition to the granular settings, a button for ‘Accept All’ and ‘Reject All’ must be provided at the first visual level. These buttons are necessary to reduce the problem of consent fatigue as long as internet users cannot use a consent agent to make granular decisions beforehand.
- All buttons must be designed to be neutral or similar in appearance, so that their design *does* not encourage internet users to click *rather* “Accept (All)” than “Reject (All)” – or reverse.

  IMPORTANT: The design of buttons that make it more difficult to refuse consent also constitutes a dark pattern, because data protection law is not about making it easier to refuse consent, but about enabling informed decisions, regardless of the position the internet users may take.



The integration of consent agents opens up new possibilities for the design of the buttons: Since internet users are able to make decisions beforehand using consent agents, thereby solving the problem of consent fatigue, the buttons can and must be designed in a granular manner both within the consent agent and in a cookie banner that communicates with consent agents. This granular design ensures that internet users make decisions for the various data processing purposes at least once.

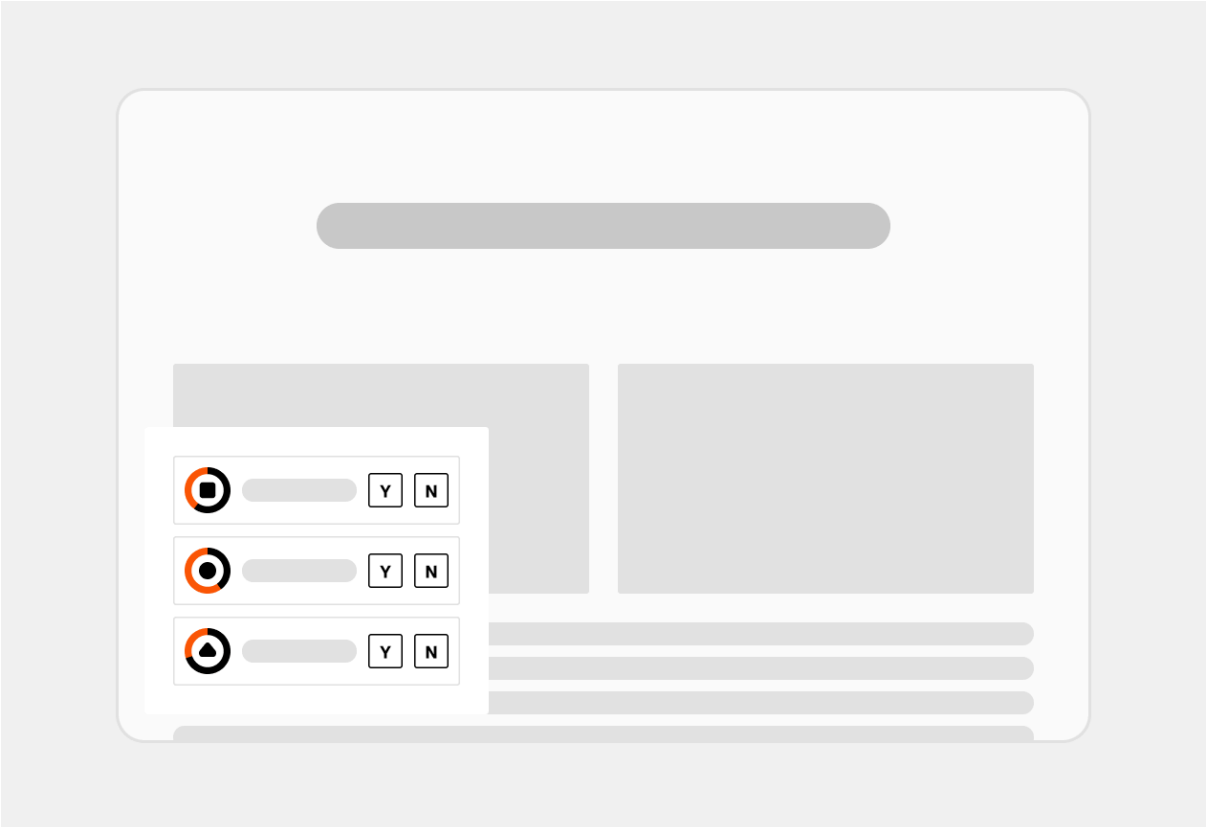
Accordingly, the following design guidelines aim to ensure that internet users make granular decisions:

- The buttons in both the consent agent and the cookie banner must not include an option to accept or reject all processing purposes wholesale. Internet users must therefore decide on a granular basis, i.e. for each individual purpose.

- The buttons in both the consent agent and the cookie banner must be set to a neutral default position. Internet users must therefore actively decide whether to consent to or object to a processing purpose.

IMPORTANT: These design requirements are subject to the condition that internet users can make these decisions beforehand using a consent agent. This is the only way to avoid the problem that these requirements would otherwise necessitate more clicks, thereby exacerbating the issue of consent fatigue. However, since internet users are able to set a default preference that applies to all websites by using a consent agent, these design requirements ensure that internet users make decisions for the various data processing purposes at least once. Provided that internet users can make these decisions beforehand with the help of a consent agent, these requirements do not constitute a dark pattern. On the contrary, they ensure that internet users make informed, conscious and granular decisions.[40]

Here, too, there is likely to be further potential for development in the state of the art. Should it be demonstrated that a different design enables even more informed and conscious granular decisions, this will represent the new state of the art.



Side note: Consent rates based on a quantitative A/B/n test

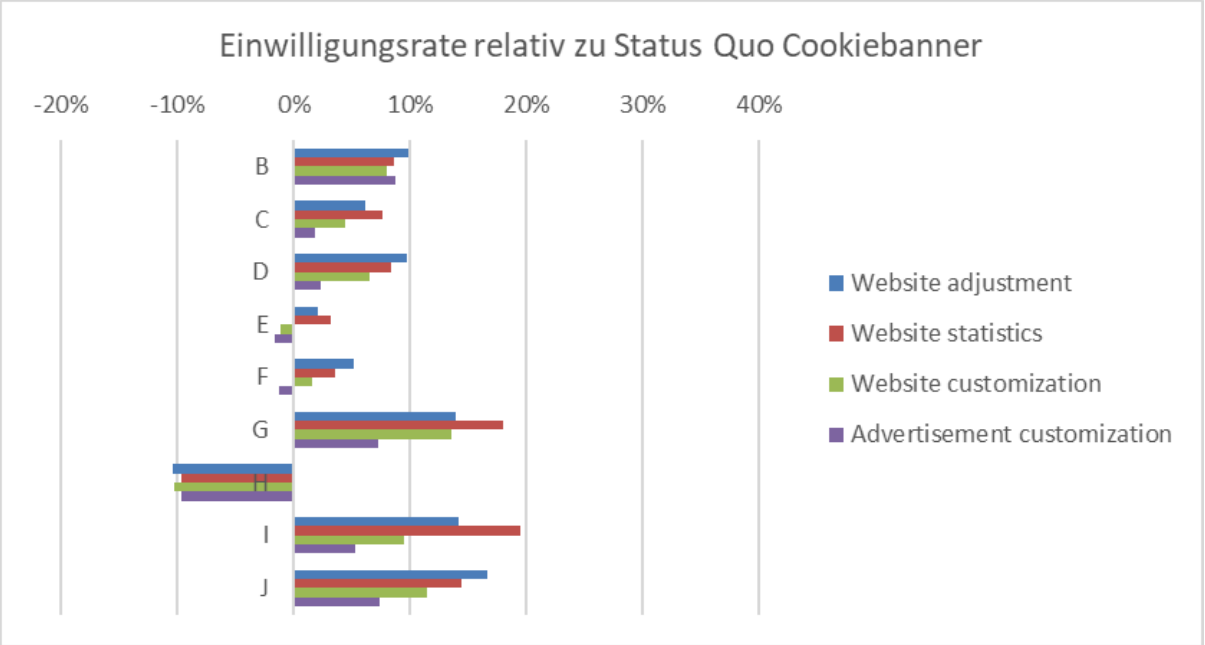
Although this is irrelevant from a data protection law perspective, we will briefly discuss the implications of the proposed ‘state of the art’ designs, as this is of practical importance to many website providers:

[40] For a distinction between dark patterns and neutral or supportive buttons, see Grafenstein, M. v., Hölzel, J., Irgmaier, F. & Pohle, J. (2018). Nudging: Regulation through Big Data and Behavioural Sciences, available at https://idw-online.de/de/attachmentdata66585.pdf.

With current best-practice cookie banners, the granular settings often lead to a drop in consent rates. The reason for this is that the granular settings are likely to overwhelm internet users.[41] However, the use of consent agents does not automatically lead to a reduction in consent rates. In fact, consent rates may even be higher compared to best-practice cookie banners. The key factor here is how the decision-making mechanisms are specifically designed (see in detail below).

This point is important because, in light of the introduction of Apple's App Tracking Transparency Framework, there are concerns within the industry that consent rates will fall with the introduction of consent agents.[42] If consent processes are designed in accordance with the conditions set out here, the involvement of consent agents generally leads to an increase in the consent rate (see study groups G and D in Annex II). This is demonstrated by the following table from a quantitative long-term field study.

Here, too, there is likely to be further scope for development in the state of the art. Should it be demonstrated that a different approach enables even more informed and conscious granular decisions, this will represent the new state of the art.



3.5 Mutual integration of the various touchpoints

To ensure that internet users are effectively informed so that they can engage consent agents when making decisions about the disclosure of their data, this information must be

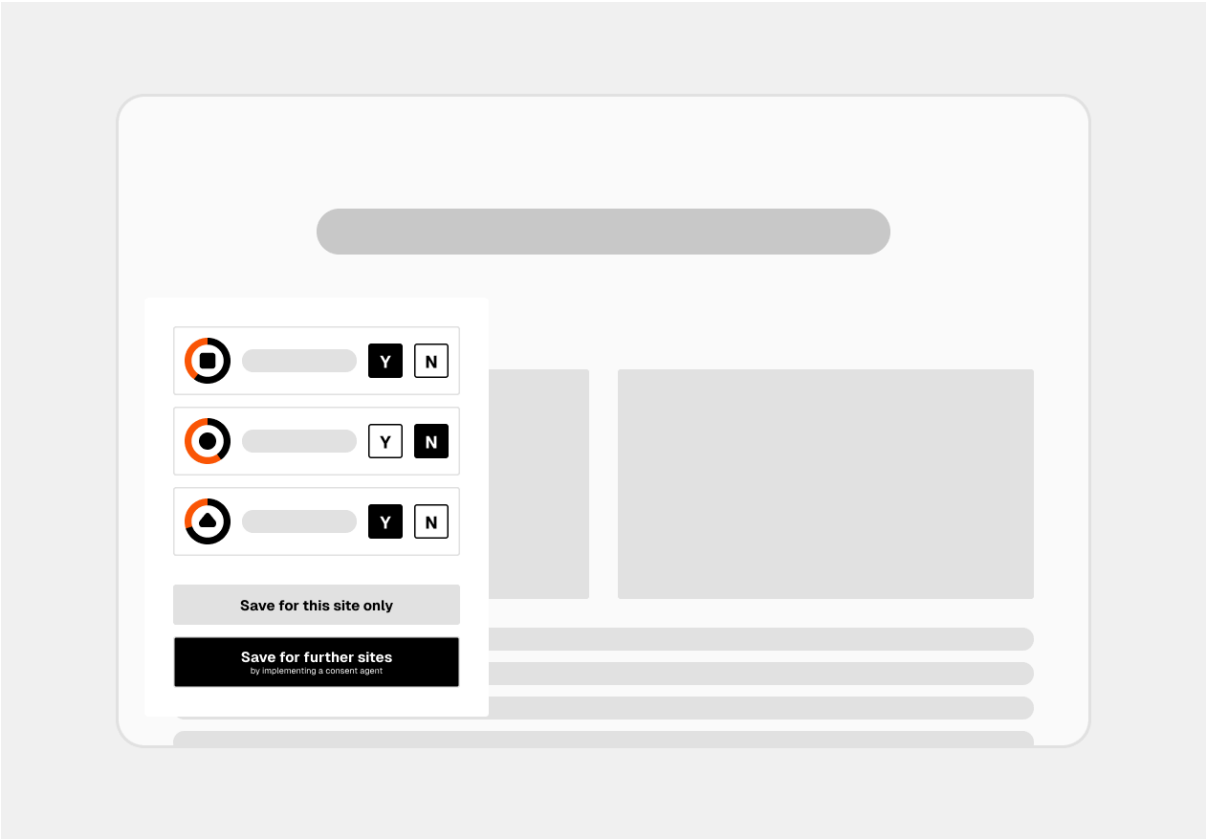
[41] Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, Proceedings of CHI '20 CHI Conference on Human Factors in Computing Systems, 25–30 April 2020.

[42] See various statements from the advertising industry regarding Article 88b (and a) of the Digital Omnibus, for example, https://www.aig-europe.eu/wp-content/uploads/2026/03/AIG-Digital-Simplification-Position-Paper.pdf?utm_source=chatgpt.com; https://ecommerce-europe.eu/wp-content/uploads/2026/03/Annex-2-ECOM-Final-Position-Paper-Digital-Omnibus.pdf?utm_source=chatgpt.com.

integrated into the appropriate usage context. The appropriate usage context is the moment when internet users have the greatest need for a consent agent, i.e. when they are suffering from ‘consent fatigue’ because they have to click away a cookie banner.

Cookie banners must therefore contain two buttons via which internet users can save their decisions for the individual processing purposes solely for the service being used at that time – or, additionally as a default setting, for all other websites or digital services by downloading a consent agent via the link provided in the second button. This link must lead to a website listing all available consent agents.

Ideally, the legislator should clarify which competent authority operates the website containing the links to the available consent agents and what requirements consent agents must meet in order to be listed.

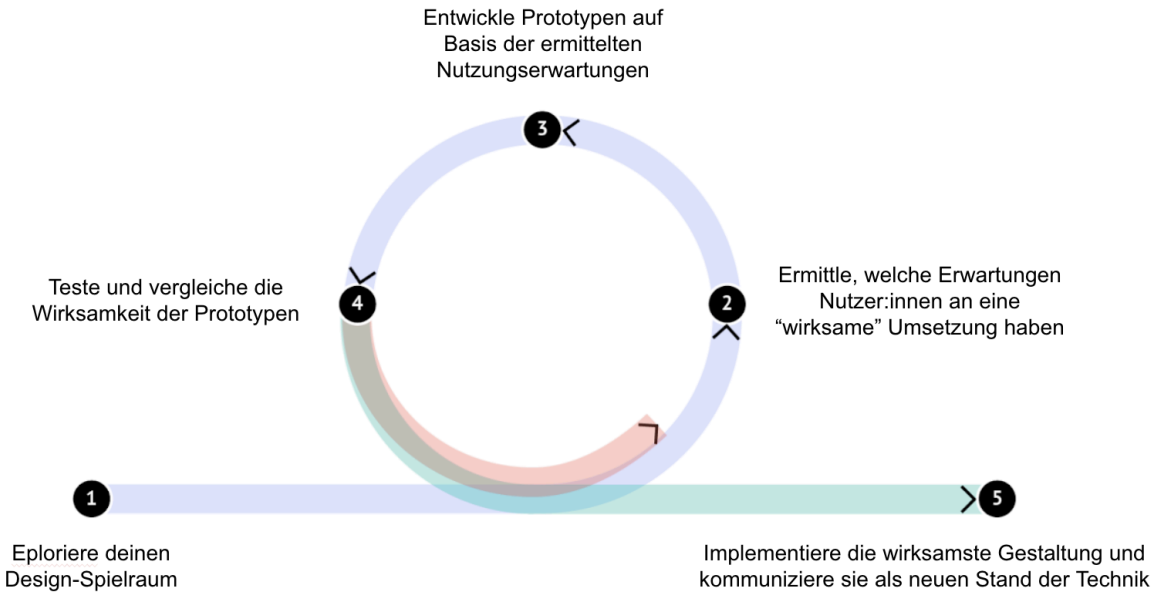


4. Empirical methods for demonstrating effective decision-making mechanisms

The previous chapter repeatedly highlighted areas in which further advancements in the state of the art are to be expected. Although the design specifications outlined represent the most effective implementation of informed consent and other decisions to date, even more effective designs are (hopefully) likely to evolve. The following iterative design process may be followed to develop decision-making processes that may be even more effective than those following the aforementioned guidelines.

4.1 Iterative design process

In brief, the process of designing increasingly effective decision-making processes can be followed over five basic steps.[43]



The first step is to define the framework for the design options. These include

- the visual conditions dictated by the specific context of use in which internet users are to be informed and make respective decisions (for example, within the context of a cookie banner, consent agent, privacy policy etc.);
- the legal requirements laid down by law;
- and the state of the art, where such a standard already exists.

If there is no state of the art yet, the controller must demonstrate that its specific implementation of informed consent is effective within the meaning of Article 25 GDPR (evidence that is rarely provided up to date). If there is a state-of-the-art solution, it makes things much easier for the controller, as it can simply replicate (or buy) it. Alternatively, the controller may also further enhance the state of the art. In the first and latter cases, the controller needs methods to evidence the (greater) effectiveness. The following brief overview of the possible methods may help the controller in doing this.

4.2 Standard: The aim is to provide effective protection against the risks of data processing to users' fundamental rights

First of all, the controller has to define the metrics against which effectiveness can be measured. As already explained, Article 25 GDPR requires a website provider to implement

[43] For details, see Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on Art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924.

informed consent, withdrawal of consent, objections and so on, in a way that provides for effective protection against the risks to the data subject's *fundamental rights*. These metrics can be divided into two basic components:

- The implementation must lead to effective protection against the respective fundamental rights risk posed by the relevant data processing.
- This effective protection must be achieved by enabling informed decisions regarding the respective processing purposes.

As a first step, therefore, the fundamental rights risks must be identified for each processing purpose and the processing operation used for this. To this end, the controller must use the standard methodologies of data protection risk assessment or data protection impact (see point 3.1 above). On the basis of the risks identified, the controller must then assess whether the respective implementation of informed consent or another decision leads to effective protection against these fundamental rights risks.

As the correct classification and weighting are crucial to the effectiveness of the protective measures, this classification process should be underpinned by appropriate methods. Ideally, a multi-stakeholder process should be carried out, involving laypeople and experts who deal with data processing practices in various fields, particularly in data and consumer protection as well as in the various – potentially competing – economic sectors (see point 3.1 above).

As already mentioned, the risks to fundamental rights largely correspond to the risk categories that even laypeople fear in relation to the use of their data. This alignment forms an important interface for determining, through further user studies, how protective measures can be designed to be as effective as possible.[44] The following chapters summarise the possible methods into three basic categories.

4.3 Qualitative studies: Why, what for – and how?

The use of qualitative research methods is well-suited to the development of effective protective measures, as they enable an in-depth understanding of the perceptions and decision-making processes of internet users. This is particularly relevant to solve the *'privacy paradox'*, whereby expressed concerns about data protection and actual behaviour often diverge.[45] The disciplines of human-computer interaction, psychology and behavioural economics, in particular, offer a rich set of methods for this purpose.

Structured interviews play a central role in this, as they can be used to explore individual attitudes, concerns and decision-making processes regarding the handling of personal data. They allow for a nuanced understanding of subjective interpretations and the often complex

[44] Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centred UX design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722.

[45] Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and Human Behaviour in the Age of Information, in: Science, Vol. 347, No. 6221, 2015, pp. 509–514; Kokolakis, S. (2017). Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon, in: Computers & Security, Vol. 64, 2017, pp. 122–134.

relationship between data protection awareness and actual behaviour.[46] Particularly in the context of 'privacy calculus', such studies demonstrate how users weigh up benefits and risks.[47]

In addition, focus groups provide valuable insights into collective patterns of interpretation and social norms. Group discussions reveal how users talk about data protection together, exchange arguments and develop positions. This is particularly relevant as privacy decisions are strongly influenced by social contexts and expectations.[48]

To understand actual behaviour in everyday life, ethnographic approaches and contextual studies are very useful. By observing the use of digital services in real-life situations, discrepancies between stated attitudes and actual behaviour can be identified. Such insights are essential for developing measures that are not only theoretically sound but also practically effective.[49] Diary studies introduce a temporal dimension, in which participants document their experiences and decisions regarding data protection over an extended period. In this way, learning processes, habituation effects and situational factors can be traced. This understanding of developmental trajectories is central, particularly for the design of sustainable privacy interventions.[50]

Finally, think-aloud studies provide direct insight into cognitive processes during specific interactions, such as when using cookie banners or privacy settings. By having users voice their thoughts aloud whilst using the interface, misunderstandings, uncertainties and decision-making logic become apparent, which must be taken into account when designing user-friendly and transparent privacy interfaces.[51]

The appropriate qualitative study design should be selected depending on the specific research question. Combining these methods yields a comprehensive picture that covers both individual and social, situational and temporal aspects of user behaviour. Such methodological triangulation is recommended if the complexity of data protection decisions is to be captured as holistically as possible.

---

[46] Cranor, L. F. (2012). Necessary But Not Sufficient: Standardised Mechanisms for Privacy Notice and Choice, in: Journal on Telecommunications and High Technology Law, Vol. 10, 2012, pp. 273–307; Nissenbaum, Helen (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford (Stanford University Press) 2010.

[47] Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, in: Information Systems Research, Vol. 17, No. 1, 2006, pp. 61–80.

[48] Nissenbaum, Helen (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford (Stanford University Press) 2010; Boyd, D. and Hargittai, E. (2010). Facebook Privacy Settings: Who Cares?, in: First Monday, Vol. 15, No. 8, 2010.

[49] Shilton, K. (2009). Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection, in: Communications of the ACM, Vol. 52, No. 11, 2009, pp. 48–53; Barkhuus, L. and Dey, A.K. (2003). Is Context-Aware Computing Taking Control Away from the User? Three Levels of Interactivity Examined, in: Proceedings of the Fifth International Conference on Ubiquitous Computing (UbiComp 2003), Berlin/Heidelberg (Springer) 2003, pp. 149–156.

[50] See Carter, S. and Mankoff, J. (2005). When Participants Do the Capturing: The Role of Media in Diary Studies, in: CHI 2005 Proceedings; Shilton, K. (2009). Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection, in: Communications of the ACM, Vol. 52, No. 11, 2009, pp. 48–53.

[51] See Ericsson, K. A. and Simon, H. A. (1993). Protocol Analysis: Verbal Reports as Data, 2nd ed., MIT Press; Nielsen, J. (1993). Usability Engineering, Academic Press.

However, it should be made clear that individual methods and studies already provide valuable contributions to the development of evidence-based effective measures.[52] It is then a separate question as to how reliable and comprehensive the respective evidence is. Thus, one has to start from the current state of knowledge, and on this basis, the evidence for an effective protective measure can be made more reliable and/or comprehensive by drawing on further studies and methods. When conducting empirical studies, the question is therefore not 'whether' but 'how', or rather, which step to take first.

4.4 Prototyping: Design options for the "how?"

Various prototypes should be developed based on the identified expectations for effective protection. To this end, data controllers may use the rich methodology set, particularly from user experience design and user interface design.

In particular, **prototyping methods** make it possible to test, evaluate and iteratively improve data protection-related design approaches at an early stage. They serve to translate abstract legal requirements into concrete, user-centred solutions.[53] In the context of data protection, prototyping is frequently used to develop **privacy interfaces** in particular – such as consent dialogues, cookie banners or dashboards – and to empirically assess their comprehensibility and impact on decision-making. Early-stage prototypes (low-fidelity), such as wireframes or click-through mock-ups, allow different design variants to be tested with users without having to implement complete systems. Later, more functional prototypes (high-fidelity) also enable the investigation of actual interaction processes under realistic conditions.[54]

Empirical studies show that even minor design decisions in such prototypes can have a significant impact on user behaviour. As described above, it has been demonstrated that the specific design of privacy notices and consent mechanisms significantly influences the willingness to share data.[55] Research into so-called 'dark patterns' also highlights that prototypical interface design can be used not only to improve transparency but also – abusively – to deliberately influence user decisions.[56] This is precisely why an evidence-based prototyping approach is crucial for developing data protection measures that are effective. By developing alternative prototypes, their respective effectiveness can be determined and compared relatively quickly.

Overall, research shows that prototyping is an indispensable tool for developing effective data protection measures. It not only enables the early identification of comprehensibility issues and perverse incentives, but also the systematic optimisation of design solutions in

---

[52] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p. 7.
[53] Schaub, F., Balebako, R., Cranor, L. F. (2017). Designing Effective Privacy Notices and Controls, in: IEEE Internet Computing, Vol. 21, No. 3, 2017, pp. 70–77.
[54] Snyder, C. (2003). Paper Prototyping: The Fast and Easy Way to Design and Refine User Interfaces, San Francisco (Morgan Kaufmann) 2003.
[55] Tsai, J. Y., Egelman, S., Cranor, L. F., Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behaviour, in: Information Systems Research, Vol. 22, No. 2, 2011, pp. 254–268.
[56] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI 2018); Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence, in: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI 2020).

the interests of evidence-based regulation and implementation of data protection law. Prototyping should therefore not be understood merely as the implementation of users' expectations within the defined design space. Rather, prototyping represents a method for generating further knowledge. It is often only during prototyping that one realises where the problem of data subjects in relation to understanding and controlling data protection risks is specifically rooted, where the challenges in implementation lie, and what alternative, more effective solutions exist that had not previously been considered.

In the end, the design options developed should always be tested for their effectiveness using qualitative methods (see previous chapter). These qualitative testing and development cycles must be repeated until at least one implementation option is available that is sufficiently validated to be effective. This model then serves as a hypothesis for the quantitative test, which validates its effectiveness on a representative basis.

4.5 Quantitative A/B/n tests: What is the most effective design?

Building on the developed and qualitatively tested prototypes, **quantitative methods** are used in privacy research to systematically compare different design variants and empirically identify the most effective design in each case. The aim is to test the hypotheses derived from exploratory studies under controlled conditions and to make robust statements about causal relationships between design decisions and user behaviour.

A key method here is **randomised controlled trials (RCTs)**, particularly in the form of A/B tests or multivariate experiments. Users are randomly assigned to different design variants – such as different cookie banners or privacy notices – so that differences in behaviour can be causally attributed to the respective design. Such approaches are widespread in privacy research and have shown that even minor changes in presentation or default settings can have significant effects on consent rates and data disclosure.[57] In addition, economic field studies highlight the importance of real-world usage contexts for evaluating such effects.[58]

In addition, **online experiments and survey experiments** are used to reach larger and more diverse samples and to examine specific influencing factors in isolation. In such studies, for example, different information presentations, framing effects or default settings can be varied and their influence on decision-making processes measured on a broader scale. Research shows that such quantitative studies are able to capture factors such as framing, timing and the context in which information is provided having a significant impact

[57] Adjerid, I., Acquisti, A., Brandimarte, L., Loewenstein, G. (2013). Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, in: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS), 2013; Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field, in: Proceedings on Privacy Enhancing Technologies (PoPETs), 2019(1), pp. 346–367; Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence, in: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI 2020).

[58] Goldfarb, A. and Tucker, C. (2012). Privacy and Innovation, in: Innovation Policy and the Economy, Vol. 12, 2012, pp. 65–90.

on privacy decisions.[59] So-called discrete-choice experiments also allow the preferences of users for various privacy features to be modelled quantitatively.[60]

Furthermore, large-scale analyses are becoming increasingly important, particularly in the context of platforms and digital services. These allow design decisions to be tested with very large user groups and also enable the observation of longer-term effects, for example with regard to user retention, trust or sustainable behavioural changes.[61] It is clear to all readers, and should nevertheless be mentioned, that such experiments must be carefully designed to meet ethical requirements – particularly with regard to informed consent and transparency.

Overall, quantitative methods enable a systematic, representative evaluation of different privacy designs and thus form an indispensable complement to qualitative approaches.[62] Whilst qualitative methods generate hypotheses and foster an understanding of context, quantitative experiments provide the necessary empirical basis for validating design decisions and translating regulatory requirements into demonstrably effective measures. On this basis, different design options can be compared and the most effective protective measure reliably identified.

Here, too, it should be clarified that even individual quantitative methods and studies make valuable contributions to evidence-based, more effective measure development.[63] Thus, the question arises, here again, as to how reliable and comprehensive the respective evidence is. The current state of knowledge must always be taken as the starting point; on this basis, the evidence for an (more) effective protective measure can then be made even more reliable and/or comprehensive by drawing on further quantitative studies and methods.

5 Outlook: The development of state-of-the-art approaches towards (ever) more effective designs

The previous remarks only provide a short overview of the diverse set of methods that can be used to ensure and demonstrate the effective implementation of informed consent and other decision-making processes. As emphasised occasionally, providers of websites and other services do not need to apply the entire set of methods if they wish to elicit an informed decision from their users. When conducting empirical studies to prove effectiveness of informed consent and so on, the question is not ‘whether’ but which step to take first.

The simplest approach for service providers is when a state of the art already exists for the processing purpose in question, the fundamental rights risks it entails, and the appropriate

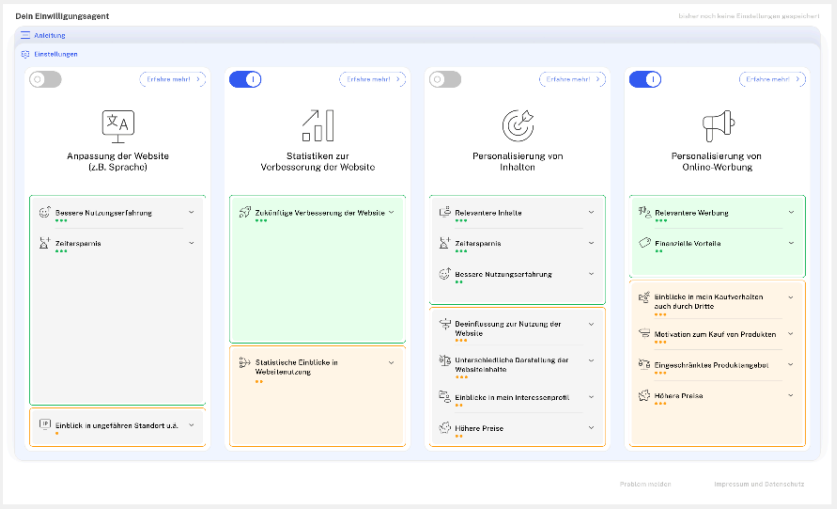
---

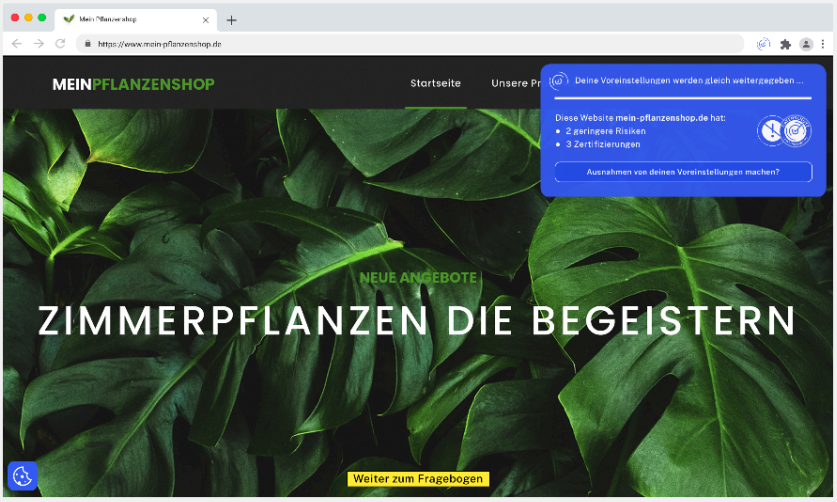
[59] Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and Human Behaviour in the Age of Information, in: Science, Vol. 347, No. 6221, 2015, pp. 509–514; Johnson, E. J., Bellman, S., Lohse, G. L. (2002). Defaults, Framing and Privacy: Why Opting In-Opting Out, in: Marketing Letters, Vol. 13, No. 1, 2002, pp. 5–15.
[60] Beresford, A. R., Kübler, D., Preibusch, S. (2012). Unwillingness to Pay for Privacy: A Field Experiment, in: Economics Letters, Vol. 117, No. 1, 2012, pp. 25–27.
[61] Goldfarb, A., Tucker, C. (2012). Privacy and Innovation, in: Innovation Policy and the Economy, Vol. 12, 2012, pp. 65–90.
[62] Acquisti, A., Taylor, C., Wagman, L. (2016). The Economics of Privacy, in: Journal of Economic Literature, Vol. 54, No. 2, 2016, pp. 442–492.
[63] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p. 7.

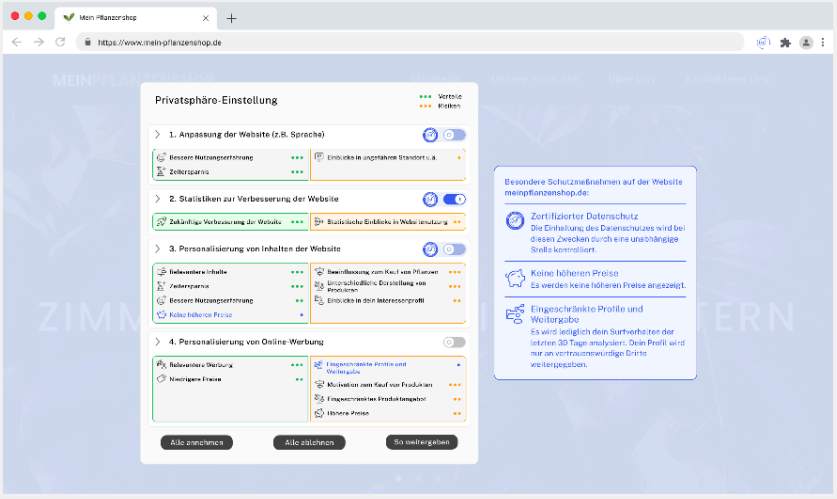
protective measure. In such cases, a data controller needs only to apply this state of the art, provided that this does not entail disproportionate costs. A separate proof of effectiveness is not required. However, a separate proof of effectiveness is required if there is no state of the art yet, i.e. no evidence of effectiveness in the relevant area in question.

In the area of informed consent and further decisions, the state of the art, as described in point 3, is now available. The methods described are therefore of particular interest to those stakeholders who wish to further develop the state of the art or extend it to other areas. Let us all work together – whether from the areas of research, business or public authorities – to unleash the market dynamics envisaged by the legislator in Articles 25 and 32 of the GDPR. A move towards ever more effective data protection.

Annex 1: Concept designs for informed consent







Annex 2 – Designs of study groups G and D in the quantitative study on consent rates