Effective regulation through design

Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking technologies in personalised internet content and the data protection by design approach

Published / version no.
23.06.21 / 1.1

Authors
Prof. Dr. Max von Grafenstein, LL.M.
Julie Heumüller
Elias Belgacem, LL.M.
Dr. Timo Jakobi
Patrick Smieskol

Keywords
ePrivacy Regulation, EU General Data Protection Regulation (GDPR), data protection by design, tracking technologies, evidence-based regulation through user-centered design

Universität der Künste Berlin
Berlin Career College

BERLIN OPEN LAB

EINSTEIN CENTER Digital Future

Table of content

Background info

This comment is based on the experiences and learnings from several research projects (being) conducted at the Einstein Center Digital Future (ECDF) affiliated with the Berlin University of the Arts (UdK) and located at the Berlin Open Lab (BOL).

Author info

Dr. Max von Grafenstein, LL.M., is full professor of the chair Digital Self-Determination at Einstein Center Digital Future and Head of Research The Governance of Data-Driven Innovation at Alexander von Humboldt Institute for Internet and Society. He is also working as an attorney at Law at iRights.Law Berlin.

Julie Heumüller has been working as a research assistant in the Einstein Center Digital Future professorship for "Digital Self-Determination" with Prof. Dr Max von Grafenstein at the Berlin University of the Arts (UdK) since January 2021. Previously, she completed her Master of Arts at the UdK in the program "Visual Communication". With her studies in the class "Visual Systems" and her master's thesis in the "Visual Society Program", her current work focuses on the interface of design and science.

Elias Belgacem, LL.M., is a research assistant in Prof. Dr. Max von Grafenstein's team at the Berlin University of the Arts (UdK) and president-founder of the Euro-Mediterranean Legal Center (EMLC). His personal research project mainly focuses on how to turn data protection (by design) legal requirements into a competitive advantage. He studied international technology law at the Vrije Universiteit Amsterdam and French and German law at the Université de Cergy-Pontoise and Heinrich-Heine-Universität Düsseldorf.

Dr. Timo Jakobi is managing director of the Institute for Consumer Informatics and head of an EU-funded PhD school on human-centric artificial intelligence at the University of Siegen. His research focuses on the exploration and development of usable support mechanisms for privacy management in ICT applications. In particular, Timo is active at the intersection of user research and legal studies to inform the definition and interpretation of (data protection) law with a robust, empirical consumer perspective.

Patrick Smieskol is a student research assistant in the Einstein Center Digital Future professorship for "Digital Self-Determination" with Prof. Dr. von Grafenstein at the Berlin University of Arts (UdK) since Dezember 2020. Simultaneously, he is finishing his Master of Social Sciences at Humboldt-Universität zu Berlin.

Citation

M von Grafenstein, et al. (2021). Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking technologies in personalised internet content and the data protection by design approach – Effective Regulation through Design. https://doi.org/10.5281/zenodo.5008420

Executive summary

After numerous revisions of the initial draft of the ePrivacy Regulation, the Portuguese presidency finally submitted a draft that all EU Member States agreed on. We would like to take the opportunity of the trilogue's beginning to point out a serious technical flaw in the current draft. This flaw lies in the ambiguous relationship between the ePrivacy Regulation and the GDPR. As such, this ambiguity calls into question the applicability of several decisive provisions of the GDPR including the data protection by design approach and co-regulation instruments such as codes of conduct and certificates.

The electronic communications sector is characterised by two key aspects in particular: a rapid pace of technological development and the dependency of users on the trustworthiness of electronic communication providers. Since third parties mediate data subjects' communication, data subjects on their own can exercise limited control over their privacy, freedom, equality, etc. Based on our interdisciplinary research focusing on personalised content and tracking technologies, we observe that the current draft of the ePrivacy Regulation does not provide a level of protection that could be considered effective in meeting the needs of electronic communications users. Effective protection could however be provided by applying the aforementioned GDPR provisions. Therefore, it would prove contradictory to legislator goals for the ePrivacy Regulation to jeopardize preexisting GDPR provisions that are best suited to meeting the needs of data subjects.

In order to avoid this ambiguity, the legislator has two options: Either the legislator may specifically clarify the application of the data protection by design approach and other related provisions (in particular the processing principles, data subjects' rights and certification mechanisms) in the ePrivacy Regulation. Or, taking on a more fundamental approach, the legislator may clarify, firstly, in Art. 1 sect. 3 that "insofar as the Regulation does not provide for more specific rules, the provisions of the GDPR shall apply". Secondly, the legislator has to clarify in the specifying provisions of the ePrivacy Regulation which GDPR provisions they refer to, and to what extent (e.g., restriction of the legal basis or of the purpose compatibility assessment); in this way, the legislator can avoid unclear specifications leading to the exclusion of GDPR standards that the legislator probably did not intend to exclude.

With this study, we would also like to recommend to the legislator an expansion of its legislative methods to include those of other disciplines such as user experience design research and visual design. While legislation should still draw from the legal considerations involved in the legislative information process, we suggest that this process would benefit considerably if supplemented with empirical studies and design methods such as those presented in this paper. Accordingly, the legislator could test which regulations produce which effects in practice, thereby increasing the effectiveness and the rationality of laws. In conclusion, we argue for more evidence-based lawmaking through design.

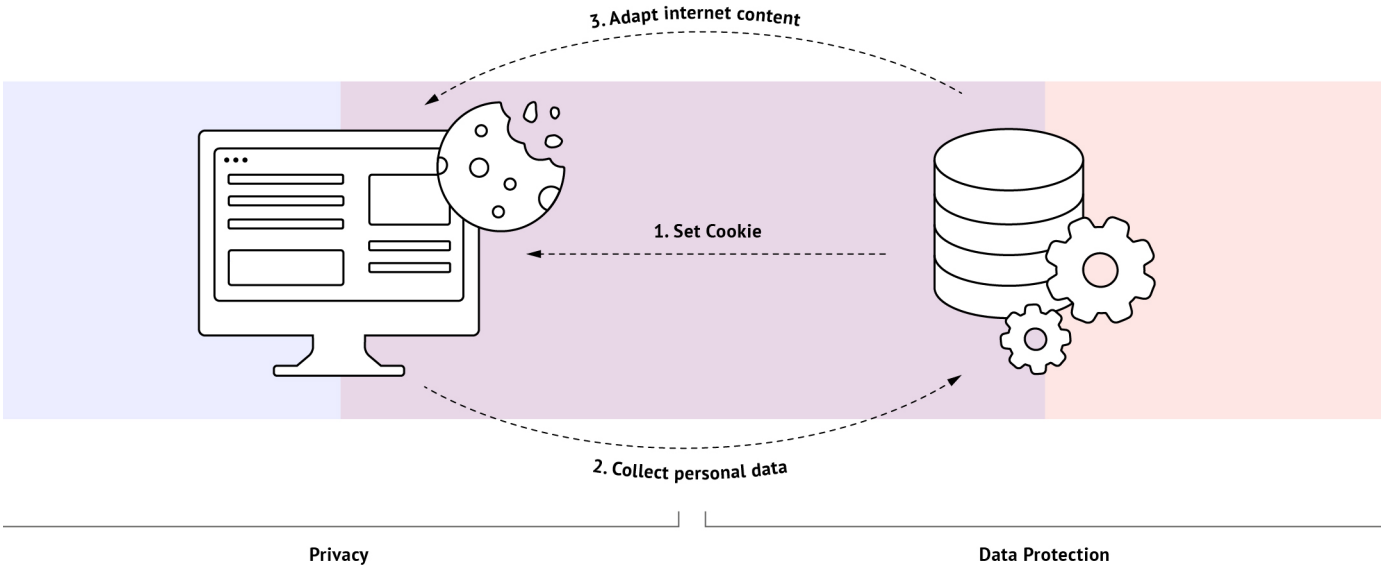
Intro: The interplay of the ePrivacy Regulation with the GDPR

In January 2017, the EU Commission presented the ePrivacy Regulation as a new legislative proposal to protect the privacy of electronic communication. This new regulation was intended to replace the ePrivacy Directive and was to come into effect alongside the EU General Data Protection Regulation (GDPR) in May 2018. However, the legislative process took a different course. After numerous revisions, the Portuguese presidency finally submitted a draft that all EU Member States agreed on; the resulting draft is the basis for the current trilogue amongst the EU Parliament, the Commission, and the Council. We would like to take the opportunity of this redrafting process to point out a serious technical flaw in the current draft. This flaw lies in the ambiguous relationship between the ePrivacy Regulation and the GDPR. As lex specialis to the GDPR (Art. 1 sect. 3), the ePrivacy Regulation is deemed to specify and complement the GDPR. According to Recital 2a of the draft, the ePrivacy Regulation "does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679". However, the next sentence of Recital 2a leads to the aforementioned problem by stating as: "If no specific rules are established in this Regulation, Regulation (EU) 2016/679 should apply to any processing of data that qualify as personal data." Thus, the problem arises in the moment when the regulation contains more specific rules, although it remains unclear to what extent these provisions concretise the GDPR. This ambiguity runs the risk of excluding certain rules of the GDPR and may therefore lower the standard of protection (even if the legislator did not intend to exclude these rules).

In our opinion, the current draft contains numerous ambiguous provisions that calls into question the applicability of several decisive provisions of the GDPR; first and foremost, the data protection by design approach and co-regulation instruments such as codes of conduct and certificates. Suppose these provisions are not applied to the processing of personal data in the electronic communications sector. In that case, it will be virtually impossible to effectively protect data subjects in step with the high pace of innovation in this area. Especially in the electronic communications sector, data subjects on their own can only exercise limited control over their privacy, freedom, equality, etc., since third parties mediate the data subjects' communication. It would therefore be contradictory for the ePrivacy Regulation to exclude the very GDPR provisions that are best suited to keep up with third party dependency and the rapid development in this sector.

A prominent example that illustrates our concerns is the data subject's consent. The latest draft of the ePrivacy Regulation, like the ePrivacy Directive, requires the consent of the data subjects as an important regulatory mechanism (see Art. 4a). However, the consent requirement runs the risk of being ineffectual for two reasons: First, consent alone cannot solve the problem of third-party dependency. Whether the providers of communication media adhere to the conditions of consent depends on the trustworthiness of the providers. A second decisive problem arises from consent fatigue,[1] a weariness that results from the frequency with which consent is requested from the data subject, and the way in which the actual design of the content is presented. Providers must therefore implement consent in such a way that data subjects can effectively make an informed choice and not simply give consent out of

1 Hanbyul Choi, Jonghwa Park and Yoonhyuk Jung, 'The Role of Privacy Fatigue in Online Privacy Behavior' (2018) 81 Computers in Human Behavior 42.



The relation and overlap of the two areas: privacy and data protection

frustration or fatalism. This regulatory goal applies in particular to cookies and other tracking technologies. In data protection law, Art. 25 sect. 1 GDPR is the key provision that focuses explicitly on the effective implementation of protection measures such as informed consent. The data protection by design approach requires that data controllers effectively implement the legal provisions in the technical and organisational design of the processing of personal data. Moreover, certification mechanisms as well as codes of conduct under Art. 40 to 43 GDPR ensure that data controllers effectively execute the conditions of consent given by the data subjects since data subjects are hardly able to verify this on their own. Consequently, the ePrivacy Regulation must clarify that these GDPR-provisions are applicable to the processing of personal data concerning electronic communication.

In principle, the approach of the new ePrivacy Regulation is reasonable. According to the EU Commission, an update to the existing ePrivacy Directive of 2002 was "needed to cater for new technological and market developments, such as the current widespread use of Voice over IP, web-based email and messaging services, and the emergence of new techniques for tracking users' online behaviour."[2] As said, as lex specialis to the GDPR (Art. 1 sect. 3), the ePrivacy Regulation is deemed to specify and complement the GDPR. Given that the protection of privacy in electronic communication and data protection intersect, applying a lex specialis principle is therefore plausible. On one hand, protections of privacy in electronic communications protect individuals against privacy intrusions when using such communication media; such protections function independently of whether or not such an intrusion is the result of personal data processing. On the other hand, data protection law applies to the processing of personal data regardless of whether this intrudes on an individual's electronic communications privacy. However, both areas of application can overlap or relate directly to one another, as in the case of cookies and other tracking technologies. Whether the client-side cookie itself is personal data is ultimately not a deciding factor for protecting user privacy in electronic communications,[3] however, it remains pertinent to point out that most information collected by cookies usually is personal data. So far, drafting the ePrivacy Regulation lex specialis to the GDPR is reasonable, since the ePrivacy Regulation is more specific in its scope. However, to shape such a lex specialis in an effective way, it is necessary to understand the conceptual differences of the overlapping

2 Council of the EU, 'Confidentiality of Electronic Communications: Council Agrees Its Position on EPrivacy Rules' <https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/> accessed 22 March 2021.

3 Verbraucherzentrale Bundesverband eV vs Planet49 GmbH (2019) ECJ C-673/17.

(or adjacent) scopes of the GDPR and the ePrivacy Regulation in more detail.

One established notion behind effective privacy protection suggests that concerned individuals should be able to put a stop to intrusions on their private sphere (the right to be left alone) regardless of whether or not this privacy violation leads to negative consequences for the individuals.[4] In contrast, data protection focuses on counterbalancing the informational power of data controllers created and bolstered by information technologies; this power imbalance can quickly lead to an undermining of rights to freedom, equality, etc. To address the risks which informational power asymmetries pose to the rights of data subjects, data protection focuses on limiting the personal data to the minimum of what is necessary for the controller's processing purpose and related transparency and intervention rights. Thus, the processing purpose plays a pivotal role in data protection – it is the basis by which data subjects can assess the consequences of intended data processing – and, if necessary, intervene in the processing of their data or in the use of the information created by this process.[5] For instance, certain tracking technologies ensure essential technical functions for a web session; however, such technologies can also be used to create profiles on the habits and interests of internet users to personalise internet content based on these profiles (e.g., in personalised advertisements, custom pricing, or targeted news).[6] The data protection by design approach under Art. 25 sect. 1 GDPR aims at implementing safeguards that effectively protect data subjects according to the respective risk at hand; moreover, certification mechanisms as well as codes of conduct under Art. 40 to 43 GDPR ensure that data controllers effectively execute such protections given that data subjects are hardly able to verify this on their own.

Based on our research focusing on personalised content and tracking technologies, we argue that the current draft of the ePrivacy Regulation itself does not provide a level of protection that could be considered effective in meeting the needs of electronic communications users. Applying certain GDPR provisions such as the data protection by design approach established under Art. 25 sect. 1 GDPR could mitigate inadequate protection and ensure that the needs of users are met. However, the ambiguity of the current draft runs the risk of excluding these GDPR-provisions.

4 Digital Rights vs Ireland (2014) ECJ C-293/12 and C-594/12, cip. 88, with further references to preceding decisions.

5 Maximilian von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II: Controlling Risks through (Not To) Article 8 ECFR against the Other Fundamental Rights (Esp. by the Principle of Purpose Limitation)' (2021) EDPL.

6 Cf. CNIL 'Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux cookies et autres traceurs', available (in French) at https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.

Our qualitative study: The users' needs regarding personalised content and tracking technologies

Over the last three years, our research has focused on developing and using methods to determine and ensure the effectiveness of transparency and control options for data subjects in accordance with Art. 25 sect. 1 GDPR. To this aim, we combine research approaches from the fields of data protection law, human computer interaction, and visual design. One essential step throughout our projects is an empirical assessment of privacy concerns and needs of users with respect to certain technologies. In our empirical studies, we typically begin with a qualitative research design; a qualitative approach allows us to explore phenomena requiring an in-depth examination of individual cases and to investigate the "whys" and "hows". Based on this qualitative research, it is possible to formulate hypotheses that can then be verified or falsified quantitatively. Accordingly, we do not set a purpose from the beginning in order to allow participants to speak freely in our user workshops and interviews. This approach allows content, problems, issues, etc. to be discovered without the preconditional framework of closed questions that can be answered with yes or no. Instead, open-ended questions are used to guide our participants through the topic area, leaving them room to articulate their own areas of concern; further, we prompt our participants in giving detailed answers and encourage them to say what they want. This approach avoids assigning an implicit value on certain responses over others; thus, participants are more likely to speak freely and share their perspectives in full.

In our first qualitative studies, we explored which data usage categories were relevant to data subjects when it came to informing themselves about privacy policies concerning processing purposes. Data controllers must specify their processing purpose(s) in their privacy policies in a way limiting how "controllers may use the personal data collected". These data use categories can therefore serve as a reference for controllers to more clearly include or exclude certain data uses in their privacy policies. Thus, our empirical study addresses a significant problem in the legal debate that has yet to offer few viable solutions: how broadly data controllers can specify their purpose? Conversely, how stringent must specifications be to comply with data protection law? Our empirical results showed that most data use categories mentioned by our workshop participants fall under the legal debate's classifications of ‚consequences' or ‚impact'. In order for purpose statements to maintain their meaningfulness, they must therefore indicate the consequences of data processing for data subjects.[7] This result falls in line with the legal debate's undisputed determination that controllers must specify their processing purposes in a way that data subjects can assess whether they find the intended use of their data „unexpected, inappropriate or otherwise objectionable".[8] Similarly, the data use categories resulting from our study can also serve as reference points for the design of privacy icons (see our visual design drafts below).

In our current empirical study, we have focused on a single concrete use case: personalised content and tracking technologies. Based on this use case and our previous research, we are now in the process of developing information and control architectures that protect users from the risks of processing

7 Maximilian von Grafenstein, Timo Jakobi and Gunnar Stevens, 'Effective Data Protection by Design through Interdisciplinary Research Methods - The Example of Effective Purpose Specification by Applying User-Centered UX-Design Methods' (in review) CLSR.

8 Art. 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 00569/13/EN WP 203.

purposes more effectively than cookie banners used in current practice. In 20 user interviews, we focused on the concerns and needs of internet users with respect to tracking technologies used to personalise content on the internet. The examples discussed with our interviewees included the personalisation of advertising, product offerings, prices, news, and electoral advertising. Discussed tracking technologies ranged from cookies to logins to newer techniques such as fingerprinting. The code set resulting from this study denotes certain significant themes, some of which were even agreed upon by all participants. Among the themes mentioned above, the following ones are worth detailed elucidation:

1. **Value of personalised content:** Users did not disapprove of personalised content in general, but rather recognised it as an important feature for businesses and themselves, since personalised content allows individuals to discover new products or find better prices and so on.

2. **"Consent fatigue" and "creepy moments":** However, users often experienced "creepy moments"[9] and "consent fatigue"[10] due to a lack of public transparency on the process behind content personalisation, the users' own ignorance of the process, and having to navigate dark pattern manipulation. Creepy moments often arose from an unexpected display of (sometimes inappropriate) content that a user attributed to their profile (and thus to their own past internet usage behaviour), but could not explain the specific connection.

    a. **Opaqueness of profiles:** Most users did not know – but some users wanted to know – why they see the content they see (i.e., how the content gets personalised). Given the example of personalised ads, users did not understand on the basis of which attributed interests the ads had been served to them and on the basis of which of their collected personal data the ad interests were attributed to them.

    b. **Users' ignorance of tracking technologies:** Another reason for creepy moments was the users' lack of understanding of how they are identified on the internet, and for whom the content is being personalized (e.g., for the user themself, their family, their flatmates). Users sharing one technical identity (e.g., via a cookie) often wonder why they can track each other's surfing behaviour via the personalised content displayed to them.

    c. **Control and deceptive design:** As soon as users understood the functionality of tracking technologies, they preferred opt-in to opt-out. Participants also wanted a general toggle button from „personalised content" to „non-personalised content" in order to understand what is visible to the general public. However, users were well aware that manipulative cookie banner design is being used online, and considered this form of manipulation very annoying.

3. **Uncertainty about concrete solutions:** While quite a few users had already slipped into a kind of fatalism and many were simply not interested in the functionality and consequences of personalised content and tracking technologies, the majority of our interviewees, however,

9 Tene Omer and Jules Poloentsky, 'A Theory of Creepy: Technology, Privacy and Shifting Social Norms' (2013) Yale Journal of Law and Technology.

10 Choi, Park and Jung (n 1).

still wanted better transparency and controls. More importantly, when asked how transparency and controls may be improved specifically, most participants were quickly overwhelmed. As a result, proposals for solutions remained largely superficial in detail; on the other hand, proposals also showed a demonstrable range in variety, ranging from better-tailored advertising to better protection of privacy and data trading.

As far as personalised content and tracking technologies are concerned, the possibility of informed consent with opt-in is obviously expected by most users (i.e. by our interviewees). The challenge, however, is not „if", but „how" informed consent with opt-in should be implemented if users are to make an informed decision on a processing operation in a given internet usage scenario.[11] The same problem arises concerning effective consent mechanisms for other tracking technologies and other processing purposes, especially if data controllers are required to present different processing purposes in a consistent and legible format from the user's perspective. Since users pursue other goals when using the internet, they allot limited attention to secondary tasks including those related to data protection. For these behavioral-economic reasons, an assortment of the variety of processing purposes, related information, and control options must be weighed and visually presented according to their level of importance. This makes lawyers and UX designers working in this field what Sunstein calls *"choice architects"*.[12] Against this background, the question is: does the current draft of the ePrivacy Regulation provide effective protection for the observed needs of electronic communication users?

11 Jan M Bauer, Regitze Bergstrøm and Rune Foss-Madsen, 'Are You Sure, You Want a Cookie? – The Effects of Choice Architecture on Users' Decisions about Sharing Private Online Data' (2021) 120 Computers in Human Behavior 106729.

12 Cass R Sunstein, 'Choosing Not to Choose' (2014) Harvard Public Law Working Paper <https://papers.ssrn.com/abstract=2377364> accessed 5 May 2021.

Does the latest draft of the ePrivacy Regulation meet the users' expectations? Hardly.

Does the latest draft of the ePrivacy Regulation address the needs for protection mentioned above? In our opinion: hardly. To substantiate this disappointing outcome, we will make our way through the regulatory thickets of the ePrivacy Regulation. As such, we will highlight the ambiguous interplay of the ePrivacy Regulation with the GDPR, and the problems this ambiguity creates when it comes to implementing effective transparency measures and controls set forth by the data protection by design approach in Art. 25 sect. 1 GDPR.

A bullet point summary of the ePrivacy Regulation's regulatory framework

The ePrivacy Regulation's entire framework is so confusingly written that even for readers well-versed draft legislation, the current draft may prove nearly impenetrable. Thus, we have taken the liberty of providing the following bullet point summary (some rules have been left out for the sake of brevity). Highlighted sections in blue restrict the data controller's legally permitted scope of action compared to the GDPR. Highlighted sections in green show clarifications or beneficial additions to provisions of the GDPR. Highlighted sections in yellow pinpoint inconsistencies within the latest draft of the ePrivacy Regulation itself. Finally, highlighted sections in red focus on problematic ambiguities regarding the interplay with the GDPR.

Art. 1–4	**1.**	**Subject matter, material, and territorial scope, definitions**
Art. 4 a	**2.**	**Consent** a. GDPR provisions regarding consent shall apply – sect. 1 → Does this mean, argumentum ex contrario, that other GDPR provisions do not apply unless they are explicitly mentioned)? b. Specifications for Art. 8 sect. 1 lit. b ("cookies", "fingerprinting", et al.) i. Data subjects may use software agents (e.g., browsers) to consent to cookies and fingerprinting; however, directly expressed consent prevails (sect. 2 and 2aa) ii. Consent shall be stored directly in the technical protocol of the data subject's device (sect. 2aa); if the provider is not able to identify a data subject, the technical protocol showing that consent was given from the device shall be sufficient to demonstrate the consent of the data subject (sect. 2a) c. Reminder of users to withdraw consent in periodic time intervals (sect. 3)
Art. 5	**3.**	**Confidentiality of electronic communications data**
Art. 6	**4.**	**Communication data (including content and metadata) – strict purpose identity** a. Permitted processing purposes (sect. 1) → fewer legal grounds than in Art. 6 sect. 1 GDPR

i. Technical service provision (lit. a)
ii. IT security (lit. b and c)
iii. Legal obligation (lit. d)

b. Requirement: Storage limitation, anonymised data must be insufficient for purpose (sect. 2) → Is this requirement looser than Art. 5 lit. c and e GDPR (since conditions of "adequacy", "relevance", and "pseudonymisation" are not mentioned)?

c. Requirement: Data processors may only process data for an electronic communication network provider in accordance with Art. 28 GDPR → Is this a clarification/specification regarding the GDPR? If it is a specification, does this condition imply the following argumenta ex contrario: 1) Do other GDPR provisions not apply to Art. 6 ePrivacy Regulation? 2) Does Art. 28 GDPR neither apply to Art. 6a–6c nor to Art. 7 and 8 (except sect. 1 lit. d and i, where Art. 28 GDPR is explicitly mentioned) ePrivacy Regulation?

Art. 6 a

5. Content data – strict purpose identity – permitted processing purposes (sect. 1) → fewer legal grounds than in Art. 6 sect. 1 GDPR

a. Consent from A and no negative effects on B (lit. a)

b. Consent from A and B (lit. b) plus the requirement to conduct a DPIA (presumably according to Art. 35 GDPR) (sect. 2) → Is this a clarification/specification regarding the GDPR? If it is a specification, does this imply the following argumenta ex contrario: 1) Do other GDPR provisions not apply to Art. 6a ePrivacy Regulation? 2) Does Art. 35 GDPR not apply to Art. 6, 6b, and 6c, nor to Art. 7 and 8 ePrivacy Regulation?

Art. 6 b

6. Metadata

a. Permitted processing purposes (sect. 1) → legal grounds more restrictive than in Art. 6 sect. 1 GDPR
   i. Network management, optimisation et al. (lit. a)
   ii. Performance of contract, billing, fraud et al. (lit. b)
   iii. Consent (lit. c)
   iv. Vital interests (lit. d)
   v. Research and statistics with location data – but no archiving – if (lit. e)
      1. pseudonymised
      2. anonymised data insufficient for purpose
      3. no profiling et al.
      4. sharing with third parties only if anonymised (sect. 2)

b. Research and statistics with non-location data – but no archiving – if the following conditions are met (lit. f) → Are the requirements for location data (lit. e) looser (except the sect. 2-requirement) than for non-location data (lit. e)? Isn't this inconsistent given that location data is typically regarded as particularly sensitive?
   i. In accordance with national law → Does this mean that a legal basis provided for by national law is required?
   ii. In accordance with Art. 21 sect. 6 and Art. 89 sect. 1, 2 and 4 GDPR → Is this a clarification/specification of the GDPR? If it is a specification, does this imply the following argumenta ex contrario: 1) If only lit. f but not lit. e of Art. 6b sect. 1 refers to Art. 21 sect. 6 and Art. 89 GDPR, does this mean that these Articles do not apply to research and statistics with location data? Thus, the data subject rights are limited when it comes to research and statistics using non-location data, but are otherwise fully applicable to research and statistics involving location data? This provision would be reasonable but should be clarified. 2) Do other GDPR provisions not apply to Art. 6b sect. 1 lit. f?

iii. Appropriate safeguards, including encryption and pseudonymisation

c. Official national and European statistics if according to national/Union law (sect. 2a)

Art. 6 c **7. Metadata purpose change**

a. Compatibility assessment (sect. 1) → Same criteria but no reference to Art. 6 sect. 4 GDPR: Is there a reason for the lack of an explicit reference?

b. Additional requirements (sect. 2) → Are these additional requirements necessary despite sect. 1, which already requires the controller to take additional safeguards into account?

i. Anonymised data insufficient for purpose and metadata erased or anonymised as soon as not longer needed (lit. a) → Is this requirement looser than Art. 5 lit. c and e GDPR (because the conditions of "adequacy" and "relevance" are not mentioned)?

ii. Obligatory pseudonymisation (lit. b) → If this obligatory specification justifies the existence of sect. 2, one should delete in sect. 1 lit. e the homologue example.

iii. No profiling et al. that produce legal effects (lit. c) → Does this mean that a controller may not originally use metadata for any kind of profiling (Art. 6b sect. 1 lit. e), but when using the metadata for a new purpose, this new purpose may include profiling as long as it does not produce negative effects for the data subjects? Isn't this inconsistent to set looser requirements for a change of purpose than for the original purpose?

c. Sharing with third parties only if anonymised (sect. 3)

Art. 7 **8. Storage and erasure of electronic communications data**

Art. 8 **9. Cookies, fingerprinting, et al.**

a. Cookies and fingerprinting (sect. 1)

i. Permitted purposes

1. Service provision (lit. a and c)
2. IT security, faults, and fraud (lit. da)
3. Software updates (lit. e)
4. Emergency calls (lit. f)
5. Consent (lit. b)
6. Audience measurement (lit. d) if on behalf or jointly with the controller (Art. 26 and 28 GDPR) → Is this a clarification/specification of the GDPR? If it is a specification, does this condition imply the following argumenta ex contrario: 1) Do other GDPR provisions not apply to this provision? 2) Does Art. 28 GDPR not apply to the other provisions of the ePrivacy Regulation unless explicitly mentioned?

ii. Purpose change

1. Compatibility assessment (lit. g) → Same criteria but no reference to Art. 6 sect. 4 GDPR: Is there a reason for this lack of an explicit reference?
2. Additional requirements (lit. h) → Are these additional requirements necessary despite lit. g, which already requires the controller to take additional safeguards into account?

a. Data is erased or anonymised as soon as no longer needed (i.)

→ Is this requirement looser than Art. 5 lit. c and e GDPR (because the conditions of "adequacy" and "relevance" are not explicitly mentioned)?

b. Obligatory pseudonymisation (ii.) → If this obligatory specification justifies the existence of lit. h, one should delete in lit. g paragraph (v) the homologue example.

c. No profiling et al. (iii.)

3. Sharing only with processors according to Art. 28 GDPR or data is anonymized → Is this a clarification/specification regarding the GDPR? If it is a specification, does this imply the following argumenta ex contrario: 1) Do other GDPR provisions not apply to Art. 8 sect. 1 lit. g and h ePrivacy Regulation? 2) Does Art. 28 GDPR not apply to the other provisions of the ePrivacy Regulation unless explicitly mentioned?

b. Data regarding network connections (e.g. wifi data, bluetooth data) – permitted processing purposes – sect. 2

i. Connection or service (lit. a and d)

ii. Consent (lit. b) if

1. Info according to Art. 13 GDPR and on how to stop collection → Is this a clarification/specification regarding the GDPR? If it is a specification, does this condition imply the following argumenta ex contrario: 1) Do other GDPR provisions (e.g. Art. 12 GDPR including section 7 on icons) not apply to the consent requirement according Art. 8 sect. 1 lit. b ePrivacy Regulation? 2) Does Art. 13 GDPR not apply to the other provisions of the ePrivacy Regulation (esp. lit. a and d) unless explicitly mentioned?

2. TOMs according Art. 32 GDPR → Is this a clarification/specification regarding the GDPR? If it is a specification, does this imply the following argumenta ex contrario: 1) Do other GDPR provisions, esp. Art. 25 GDPR, not apply to the consent-requirement according Art. 8 sect. 1 lit. b ePrivacy Regulation? 2) Does Art. 32 GDPR not apply to the other provisions of the ePrivacy Regulation (esp. lit. a and d) unless explicitly mentioned?

iii. Statistical purposes limited in time and space (lit. c) if

1. Info according to Art. 13 GDPR and on how to stop collection → Is this a clarification/specification regarding the GDPR? If it is a specification, does this condition imply the following argumenta ex contrario: 1) Do other GDPR provisions (esp. Art. 21 GDPR) not apply to this legal ground according Art. 8 sect. 1 lit. c ePrivacy Regulation? 2) Does Art. 13 GDPR not apply to the other provisions of the ePrivacy Regulation (esp. lit. a and d) unless explicitly mentioned?

2. TOMs according Art. 32 GDPR → Is this a clarification/specification regarding the GDPR? If it is a specification, does this condition imply the following argumenta ex contrario: 1) Do other GDPR provisions, esp. Art. 25 GDPR, not apply to this legal ground according Art. 8 sect. 1 lit. c ePrivacy Regulation? 2) Does Art. 32 GDPR not apply to the other provisions of the ePrivacy Regulation (esp. lit. a and d) unless explicitly mentioned?

The blue bullet points in the previous summary show the basic approach of the ePrivacy Regulation, which, as with the still applicable Directive, ultimately amounts to a limitation of the permissible legal bases and strict purpose identity (i.e., exclusion of a change of purpose). In particular, the restriction of the legal bases compared to the GDPR results in an exclusion of the „legitimate interests" of the data controller as a legal basis (cf. Art. 6 sect. 1 lit. f GDPR). However, at least the requirement of purpose identity is loosened in the ePrivacy Regulation compared to the Directive. Now, metadata (Art. 6c) and data collected in connection with cookies and fingerprinting technologies (Art. 8 sect. 1) can also be processed for another purpose outside of the initial collection purpose if the new and initial purposes are compatible. This purpose compatibility assessment in itself is not the subject of our criticism (apart from further areas which we will leave out of the discussion here for reasons of space, in particular Art. 7 of the ePrivacy Regulation). Rather, our criticism of the content begins with the numerous inconsistencies that already arise from the internal regulatory framework of the draft ePrivacy Regulation, as highlighted in yellow. Looking beyond these glaring inconsistencies, there is, however, the more significant issue of the ambiguous interplay between the GDPR and ePrivacy Regulation.

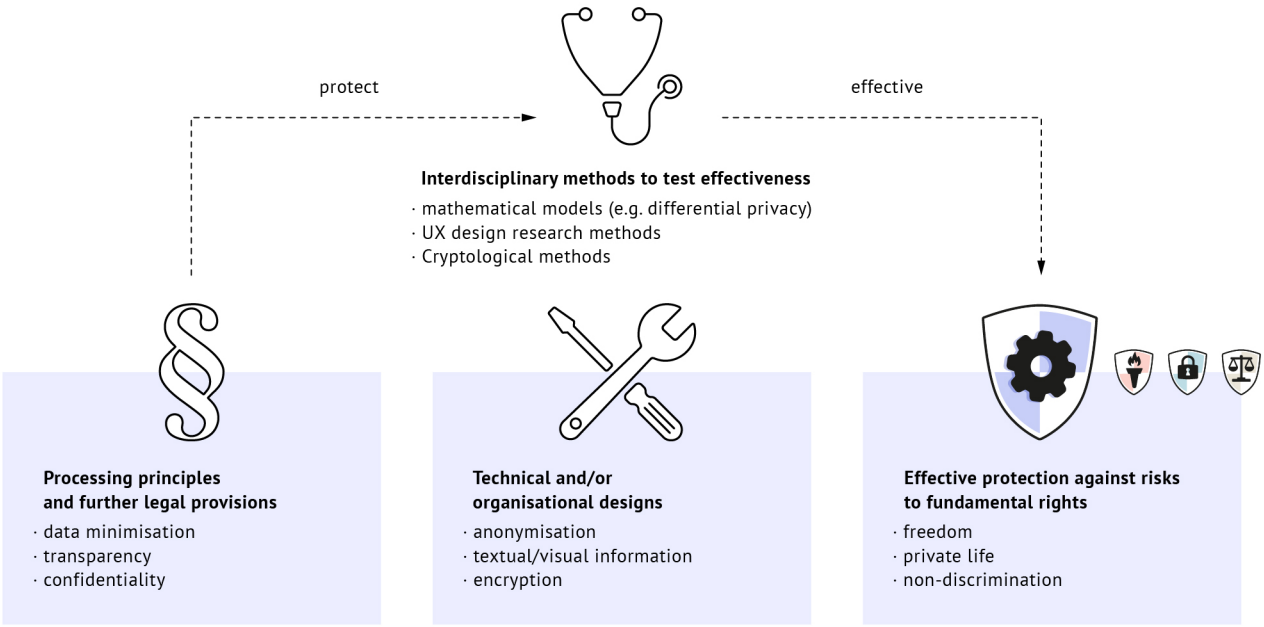
The unclear relationship between the ePrivacy Regulation and key GDPR provisions: esp. the data protection by design approach

The framework of the ePrivacy Regulation begins with a promising start. For instance, Art. 4a refers to the applicability of the corresponding GDPR provisions concerning the consent of the data subjects. The Directive adds the following few but useful clarifications highlighted in green: The periodic reminder of users to withdraw consent (Art. 4a sect. 3) is a promising instrument to make this intervention mechanism more effective in practice. The possibility to give one's consent via software agents will also contribute a lot to effectiveness (Art. 4a sect. 2) without a formal effectiveness requirement having to be mentioned in the ePrivacy Regulation itself. However, the next provision clarifies that direct user consent should prevail over consent given in advance by a software agent (sect. 2aa). At the latest in this context, the question arises as to how to design such iterative consent mechanisms to support data subjects in their decision for or against a processing purpose rather than serving as sources of confusion or annoyance. The same question arises with the subsequent provision (sect. 2a). Our interview results showed that very few users understand how they are identified through tracking technologies on a technical level. If a user is now included in the consent given by another person with whom they share a technical identity, how must these users be informed to understand the situation?

Even more problematic are the uncertainties regarding the interpretation of the ePrivacy's interplay with the GDPR (highlighted sections in red). These uncertainties are especially evident in Art. 8 sect. 2 of the current ePrivacy Regulation draft regarding the collection of data that a device exchanges with another device or network to establish the connection (e.g. via WiFi or Bluetooth). In contrast to Section 1 (which regulates the use of cookies and fingerprinting), Section 2 requires, regarding the user's consent and the legal basis for statistical data processing, that the data controller provide a clear and prominent notice according to Article 13 GDPR and apply security rules in Article 32 GDPR. As with many other references of the ePrivacy Regulation to the GDPR before, the question here is whether two reverse inferences (argumenta ex contrario) should be drawn from this reference: 1) Are Art. 13 and 32 GDPR inapplicable to other provisions of the ePrivacy regulation? In particu-

lar, since Art. 8 sect. 1 does not explicitly mention these GDPR provisions, do controllers not have to likewise inform users about cookies and fingerprinting (and to apply security measures according to Art. 32 GDPR)? 2) Conversely, does this reference also mean that the other GDPR provisions do not apply to Art. 8 sect. 2? In particular, since Art. 25 GDPR is not mentioned in addition to Art. 32 GDPR, is the data protection by design approach therefore excluded? If these conclusions are not the intention of the legislator, what is the added value of these references to the GDPR?

There are a number of other references to the GDPR and corresponding provisions in the current draft where similar questions of interpretation arise concerning the interplay between the ePrivacy Regulation and GDPR. Some examples of issues include questions of anonymisation and pseudonymisation, the purpose compatibility assessment, the design of multi-party processing and attribution of the respective legal responsibilities (processor and/or joint controller), and the data protection impact assessment. In all these cases, the same question arises as to what extent these provisions have a clarifying/specifying function. If these references have a clarifying/specifying function, what is the clarification/specification? In our view, each of these references suggests the above argumenta ex contrario. While the ePrivacy Regulation's clarification of the GDPR can at least be said to increase legal certainty of the principles set forth by GDPR, the argumenta ex contrario would prove deadly to the effective protection of data subjects in the communications sector. This result can be demonstrated clearly with respect to the data protection by design approach and related provisions.

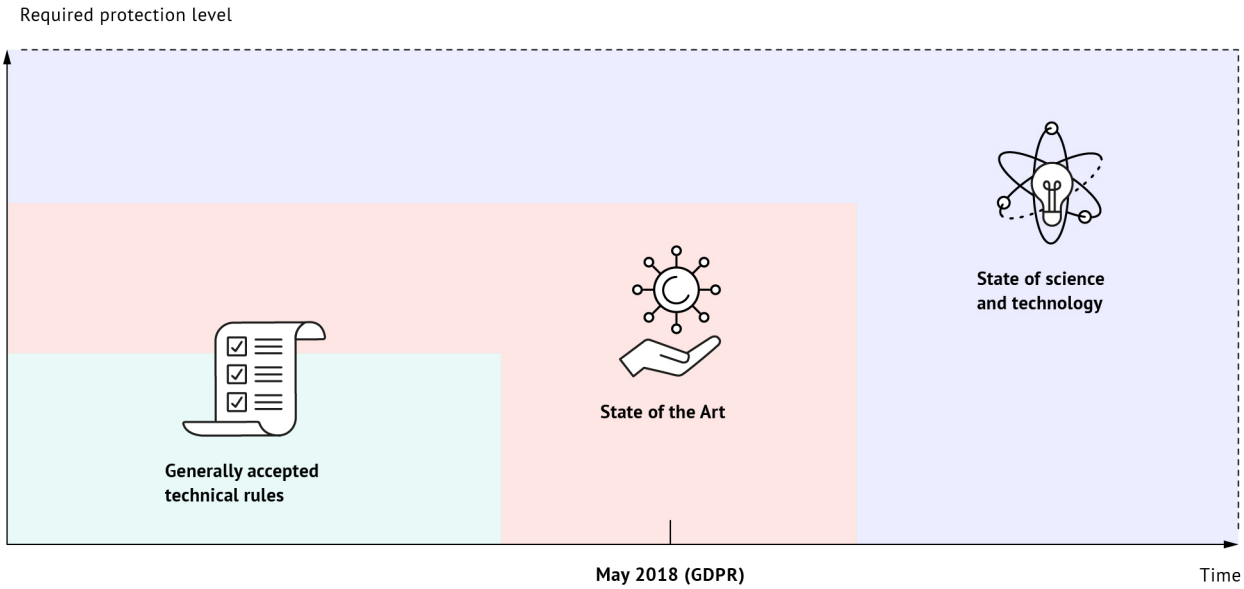


The data protection by design approach according to Art. 25 sect. 1 GDPR

The central role of the data protection by design approach for effective transparency and control measures

As mentioned above, Art. 25 sect. 1 GDPR obliges the data controller to implement the provisions of the GDPR in the technical and organisational design of its data processing in a way that effectively protects the data subjects' fundamental rights against data processing risks. Particular attention must be paid to the systematic interpretation of the provisions to be implemented in the

processing design. These provisions to be implemented include the processing principles set forth in Article 5 as well as the following statutory rules that further specify the processing principles. The interplay between these two regulation instruments (i.e. legal principles and legal rules) is important because each instrument complements one another in their protective effects. On the one hand, legal principles represent so-called optimisation standards: such standards are particularly suitable for rapidly developing areas such as the communications sector because they open up considerable scope for implementation.



The requirement of state of the art compared to the state of research and technology and the generally accepted technical rules

However, the downside of legal principles is that they provide for little legal certainty. A law may therefore compensate for the legal uncertainty associated with legal principles by concretising legal rules in addition. For example, the GDPR implements additional legal rules to bolster its processing principles by specifying the principle of lawfulness via the legal bases listed in Art. 6 (see also Art. 44 et seq.); the principle of transparency is concretized, among other things, via the information duties in Art. 12 to 14, etc. On the other hand, interpreters of the law may refer to the processing principles with their optimisation function if there are gaps between the legal rules or if the legal rules themselves are in need of interpretation.[13] Thus, applying processing principles listed under Art. 5 GDPR to the ePrivacy Regulation can help to close gaps left open by provisions of the ePrivacy Regulation, and support the interpretation of broad legal terms.

Equally important is the effectiveness requirement of Art. 25 sect. 1 GDPR. The term "effective" applies to the real-life impact of the implemented protection measures in the legal assessment: such protection measures thus typically require non-legal methods to test their effectiveness.[14] A well-known example is the use of mathematical-statistical methods to determine whether anonymisation or encryption procedures implement the data minimisation or confidentiality principle so that these principles effectively protect the privacy of data subjects. In contrast, if the effectiveness of protection measures depends on their comprehensibility and usability from a data subject perspective, as in the case of transparency measures and controls, this cannot be proven by mathematical-statistical methods, but rather with methods from UX or Hu-

13 Further references at Maximilian von Grafenstein, '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 G González-Fuster, R van Brakel and P De Hert (eds), Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, (Edward Elgar Publishing 2021).

14 EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, Adopted on 20 October 2020' cip. 7. Art. 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2017) 17/EN WP260 rev.01 13.

man-Computer Interaction (HCI) research. These UX or HCI methods can also be used to determine whether certain icons, texts, or information and control architectures protect data subjects better from data protection risks than, for instance, current cookie banners do. Subsequently, if one can reliably determine the effectiveness of certain protective measures, the state of the art can be established based on this determination. According to Art. 25 sect. 1 of the GDPR, not only must controllers implement the protection measures effectively, but also take the state of the art into account. The state of the art is understood in the GDPR as the best technology available on the market,[15] which in the sense of the above considerations means: the most effective technology available on the market. In other words, if an icon, text, or information and control architecture turns out to be the most effective measure, this tool represents the current state of the art – until an even more effective implementation of the GDPR regulations emerges.

15 Ulrich Baumgartner and Tina Gausling, 'Datenschutz Durch Technikgestaltung Und Datenschutzfreundliche Voreinstellungen' (2017) Zeitschrift für Datenschutz 311; Maximilian von Grafenstein, '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-De- sign', ibid.

Our preliminary design study: Designing effective transparency and control architectures for cookie banners (including privacy icons)

Using tracking technologies as an example, the following preliminary design study is intended to illustrate the significance of the data protection by design approach for the effectiveness of transparency measures and control options. The design study reproduces the click path of a website's users. In the text boxes, we point out the extent to which the ePrivacy Regulation prescribes or leaves open the design options discussed in our study. As far as the regulation does not prescribe explicit design options and leaves design choices open to variation, the more effective design options could only be enforced via the data protection by design approach. It is important to note that the following design study is an excerpt from a larger study: having just returned the first interim results of the visual design phase, the study is still in its beginning phase. Consequently, our designs are not yet finalised, especially in the case of icons produced by this initial study.

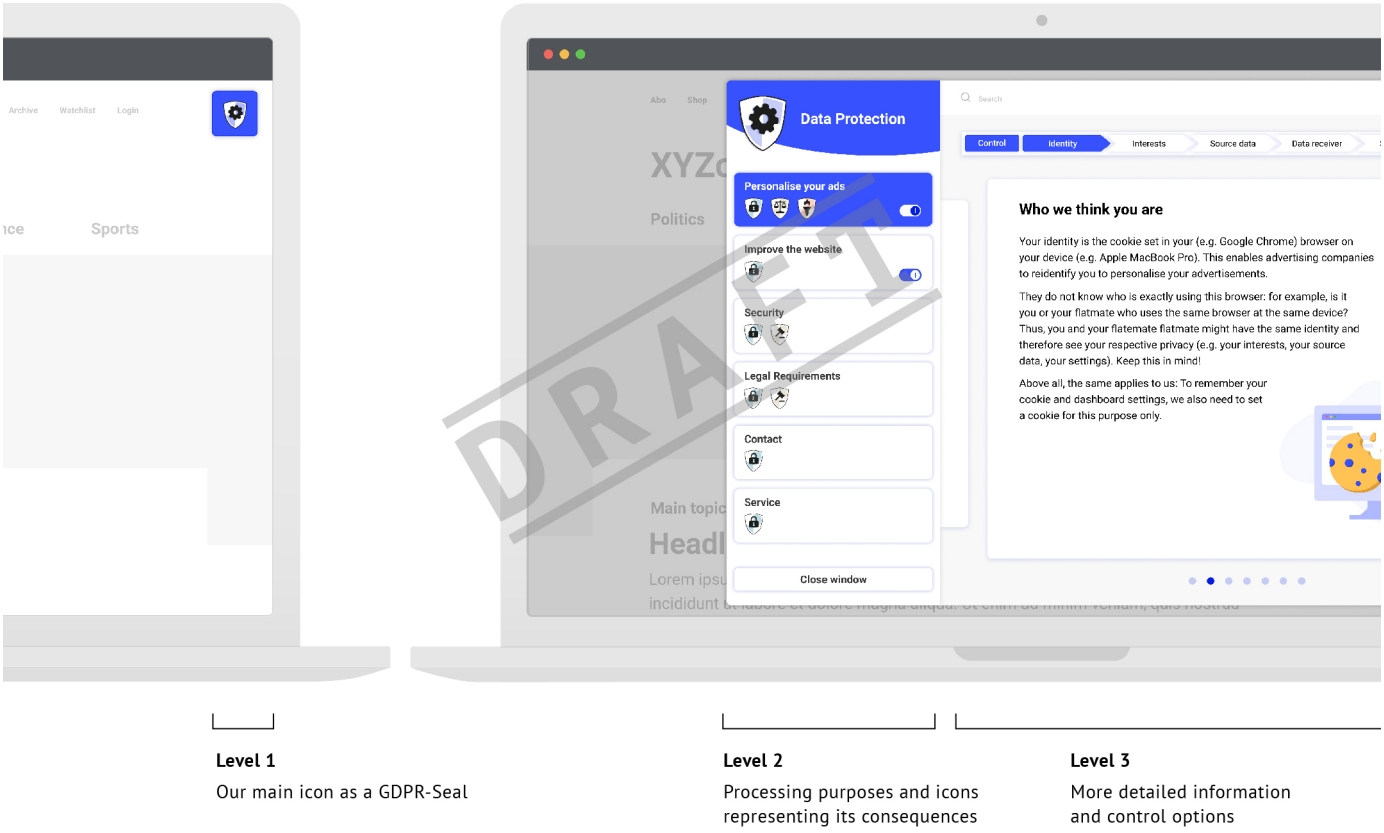


Fig. 1: Structure of our information architecture in three levels

Fig. 1: General structure

In our design study, we have decided on using privacy icons as "eye-catchers" and a "layered approach" to present privacy notices and control options. The use of privacy icons and a layered approach is not mentioned in the current

draft of the ePrivacy Regulation. However, the effectiveness of our approach (or similarly effective ones) could be tested and, in the case of positive results, enforced in practice based on Art. 25 sect. 1, Art. 5 sect. 1 lit. a and Art. 12 GDPR.

Fig. 2: Example of a website with only session cookies

Fig. 2: Session cookies

In the first use case, the website only uses session cookies (i.e., necessary to provide the service). In our legal opinion, users should not have the right to consent or object to session cookies that are necessary for website functionality and typically carry minimally invasive consequences for data subjects. A banner for these cookies is not necessary either. Therefore, users on this website are only shown the main icon, which, however, allows users to actively click to access levels 2 and 3 below.

Our privacy icons form a seal within the meaning of Art. 42 GDPR. The idea behind this is that the use of icons must be secured by appropriate certification procedures in order to avoid possible misuse (= false declaration) and thus ensure the trustworthiness of the seal in the long term. The current draft of the ePrivacy Regulation does not mention certification mechanisms, however, such mechanisms are necessary to ensure that controllers adhere to the processing conditions described in their privacy statement.

Fig. 3: Example of a website with functional and marketing cookies

Fig. 3: Functional and marketing cookies

In the following use case, cookies are set for the purposes of audience measurement and personalised advertising. Both types of cookies are more intrusive than session cookies. Therefore, information about these purposes are displayed automatically when the website is called up. Since marketing cookies imply more serious consequences for the data subjects than functional cookies, the information about marketing cookies appears at the top of level 2 upon the user's initial engagement with the website. Importantly, the toggle button for the marketing cookie is set to "off" by default, while the toggle for the functional cookie is set to "on". It is important to note that the current draft of the ePrivacy Regulation does not require that a certain order of information be presented to users. Additionally, nowhere does the ePrivacy Regulation state that users have to be informed about audience measurement cookies, let alone that they have an opportunity to opt-out.

Both processing purposes are described via the prevailing textform while additional icons represent the potential consequences of these purposes for the data subjects. The consequences for the data subjects' privacy are represented via the privacy icon with the lock. The lock is intended to reflect the concept of respect for privacy, according to which other persons can be locked out from (i.e. permitted or denied access to) one's own privacy. Not only does personalised advertising have a greater impact on privacy due to profiling, but also poses a threat to users' freedom of decision and discrimination. The possible manipulation of purchasing decisions through personalised advertising poses a threat to the users' freedom of decision. Additionally, the potential for discrimination increases when users are shown different advertisements and treated differently by consumer markets. The icons produced in this study represent these (more or less severe) additional risks with the scale and the flame of freedom. Again, the current draft of the ePrivacy Regulation does not mention privacy icons or other transparency measures to be provided in a "concise, transparent, intelligible and easily accessible form", similar to Art. 12 (esp. sect. 1 and 7) GDPR, nor in an effective manner as required by Art. 25 sect. 1 GDPR.

Fig. 4: Example of labeling for personalised advertising with our main icon

Fig. 4: "Banner Advertising"

To better meet the needs expressed by our interviewees, our protection aims at minimising the manipulation risk of personalised advertising through our main icon displayed in the banner advertisement's corner. By clicking on this icon, users can go directly to their profile in level 3. Level 3 informs users about their advertising profile: for instance, users can see what personal data was collected in order to assign the resulting attributed interests in the personalised advertisement at hand. Thus, users can understand the personalisation of advertising according to their concrete usage context and thus maintain their autonomy in their purchasing decisions. The information is also intended to avoid so-called "creepy moments" mentioned previously in our qualitative research. The current draft of the ePrivacy Regulation does not require a certain level of detail of the information given to the data subjects nor a certain usage context for placing the information. As long as the law does not require effective information and control architectures that favour better comprehensibility and usability, it can be assumed that they will not be implemented in practice on a broad scale.

Fig. 5: Automatic display of both processing purposes when the user accesses the website

Fig. 6: When the user clicks/scrolls on the website, the banner for audience measurement automatically disappears, while the personalised advertising banner is sticky

Fig. 5–6: "Nudging" – first nudge

Our protection system enables the data subjects to control the actual risks of the marketing cookie in detail on level 3. Therefore, we provide for three so-called nudges to prompt the users to level 3. Nudges serve as a design mechanism to overcome behavioral biases, such as the default bias. Since the toggle is set to „off" by default, users tend to not set the toggle to "on" simply because changing this setting requires an action that contradicts the inertia of maintaining a current state. Because we want to bring about a user decision motivated by reasons of content rather than inertia, we try to nudge users to engage with the content of consent. Whether this is good or bad nudging is both an empirical and a values question. The current debate about opting in or

opting out is being conducted in a rather superficial and binary way: in our view, this oversimplification falls short of both the conceptual claim of autonomous decision making and today's technical and methodological possibilities. In this sense, the following design options are to be understood as examples that require further detailed evaluation and will continue to be examined in further stages of our research.

When users click on or scroll down the website, the reference to the purpose "Improve the website" automatically disappears on level 2. The purpose for personalised advertising, on the other hand, only disappears when the user clicks on the exit-button ("x") provided for this purpose in the top left corner of the banner.

Fig. 7: Information displayed when the user hovers over the purpose "Personalise your ads"

Fig. 7: Second and third nudge

If the user moves the mouse over the white area, a message appears: "You're annoyed by cookie banners? Click here and control once." The settings are saved (via a separate cookie or login – corresponding information is provided on level 3) so that the banner no longer appears in future sessions; however, when visiting websites in future, the users may always reach through by clicking the main icon at the top right corner of the website to levels 2 and 3 to adjust their settings at any time.

By clicking on the blue box, users automatically give their consent. So when they get to level 3, the toggle is set to "on". Whether or how well (or badly) the information and control architecture presented here effectively empowers users to make a genuine decision for or against setting marketing cookies for personalised advertising needs to be tested empirically. However, the current draft of the ePrivacy Regulation does not make any statements on the use of good or bad nudges (i.e. "dark patterns"). Assessing such nudges legally would be possible on the grounds of Art. 25 sect. 1 GDPR.

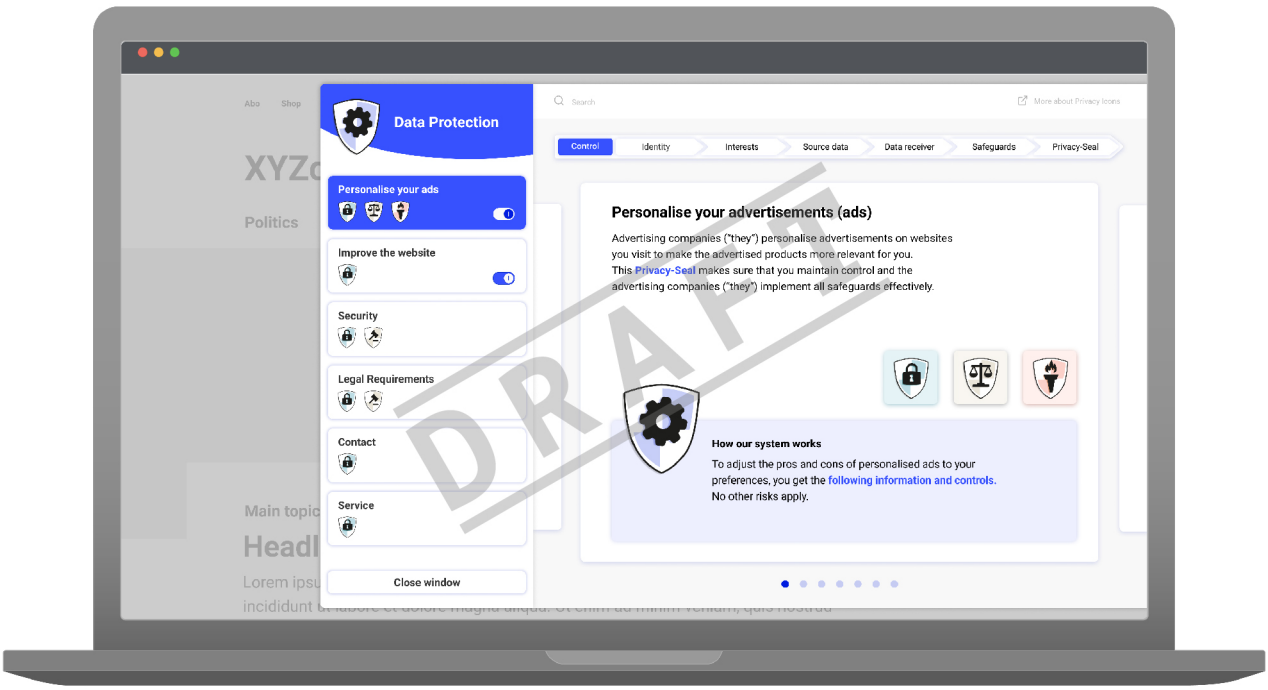


Fig. 8: Oversight tile displayed when the user accesses the third level: the privacy dashboard

Fig. 8: Our Dashboard

When users access level 3 – in our case, either by clicking at level 2 on the blue box displaying the personalised advertising purpose or clicking on the icon in the top right corner of the displayed banner advertising – they arrive at their privacy dashboard. In this dashboard, users can obtain all information according to Art. 13 and 14 GDPR and exercise their data subject rights according to Art. 15 to 21 of the GDPR. The effectiveness of implementing the aforementioned GDPR provisions is based on the concept that information and data subjects' rights are made available according to the specific usage context. The data subjects thus shall receive the information and intervention rights when they are most relevant for them. At the same time, the information and control architectures on levels 1 to 3 are designed in such a way that they should interfere as little as possible with the user's primary experience of using the website. We argue that the current draft of the ePrivacy Regulation is insufficient in this regard: In our opinion, the regulation leaves it unclear whether the information duties and data subject rights set forth by Art. 12–21 of the GDPR apply or not. In addition, the ePrivacy Regulation leaves it unclear how these duties and rights should be implemented effectively. Such an effective implementation of transparency and controls would be possible on the grounds of Art. 25 sect. 1 GDPR.

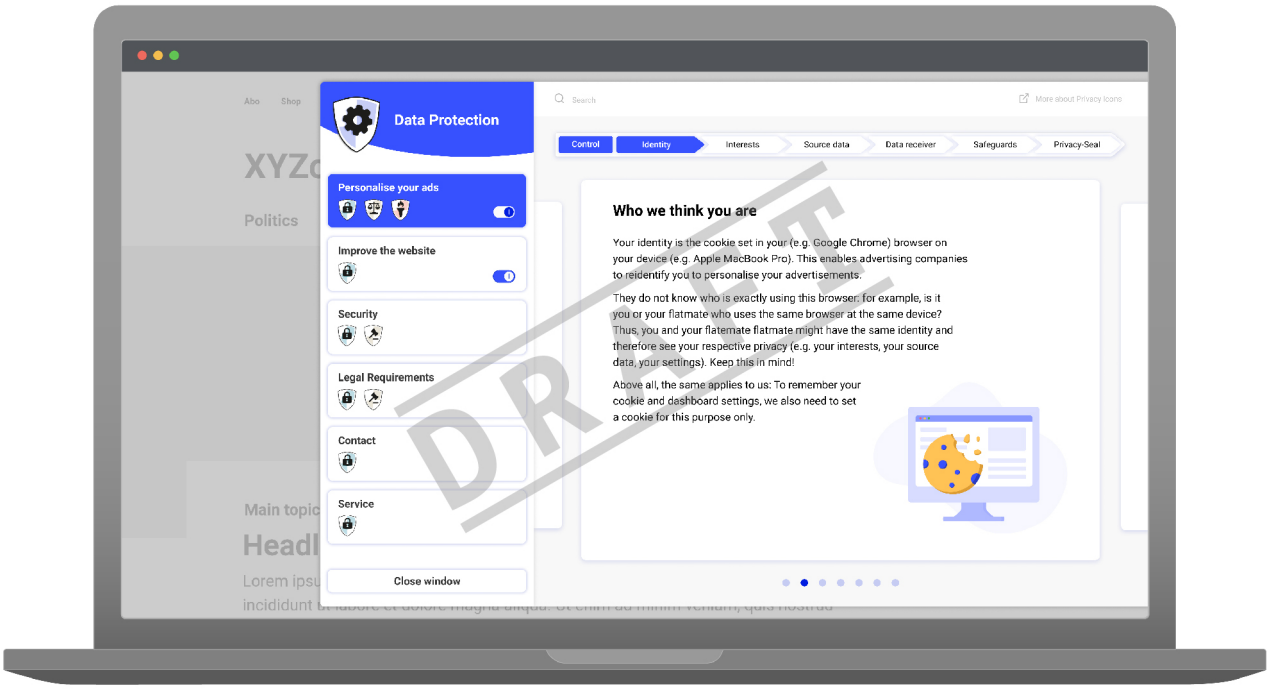


Fig. 9: With the help of a navigation bar, the user can click through information on the third level about his technical identity, related interests, data bases, etc.

Fig. 9: Identity-Screen

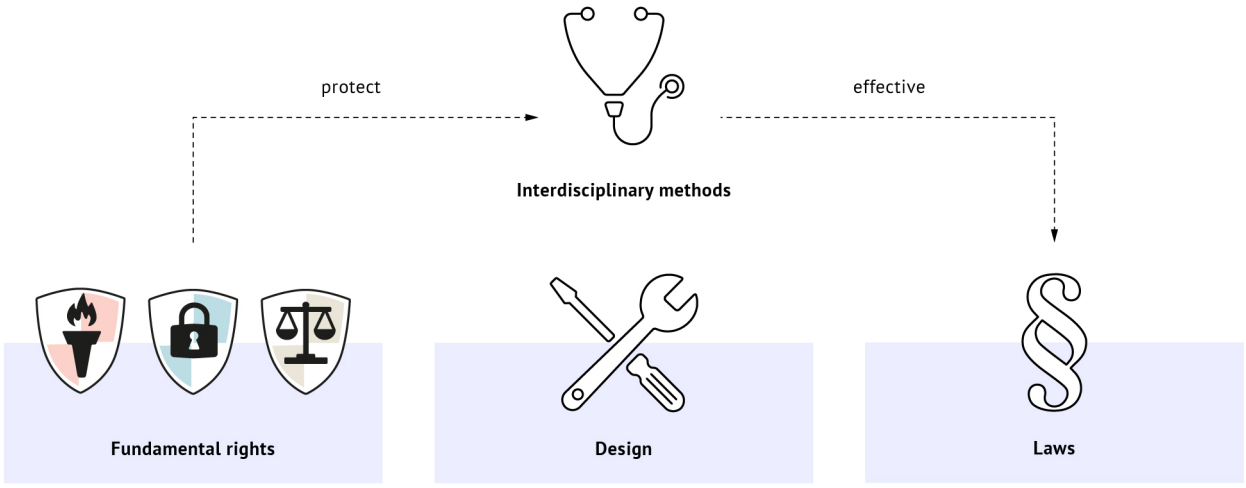
In our preliminary design study, the information and intervention options for the users on level 3 are organised via sliding tiles. A progress bar indicates the user's current location. On the second tile, users get information about their technical identity, including how they are identified by both advertising companies as well as our privacy dashboard (to save the settings for future sessions). In a philosophical sense, the concept of identity naturally encompasses the entire human being. This understanding means that the attributed interests and source data would also fall under such a broad conception of identity. However, this study concerns a narrower view: which technical characteristics are used to identify data subjects on the internet? On this tile, we give the example of cookies. The ePrivacy Regulation recognizes the problem of the ambiguous assignment of a technical identity (e.g., a cookie) to a real user. However, it does not contain any regulations on how users should be informed about this so that they can assess the consequences for themselves. Comprehensive information about the processes of technical identification would be possible on the grounds of Art. 25 sect. 1, Art. 5 sect. 1 and Art. 12 et seq. GDPR.

Conclusion: Effective regulation through design

The extracts presented from our design study were intended to illustrate possible transparency measures and control options that meet user needs concerning personalised content and tracking technologies. Whether the measures presented are more effective in meeting the expectations of electronic communication media users regarding the use of cookies (or other tracking technologies) than prevailing cookie banners requires further empirical testing. In addition, we pointed out the extent to which the current draft of the ePrivacy Regulation meets the users' needs for protection. In particular, we summarised to what extent the current draft meets the privacy measures outlined in our design and where the ePrivacy Regulation fails to provide a detailed outline or runs the risk to entirely exclude necessary GDPR-transparency measures and control options for data subjects. The same problem applies to similar privacy measures (with the same privacy intentions), which are equally relevant for our legal analysis (our own design study is, as previously mentioned, only one potentially viable model).

At least with particular respect to personalised content and tracking technologies, the current draft hardly meets the users' needs. The draft regulates, for instance, **whether** consent of users is necessary. However, the draft does not address any of the subsequent questions of **how** users should be informed and how accessible the means of consent should be in order for users to make informed decisions for or against tracking and corresponding purposes. Worse, we consider the effective implementation of transparency measures and control options (comparable to our own drafts) unlikely if the current draft of the ePrivacy Regulation does not clarify its exact interplay with the GDPR. In our opinion, most of the aforementioned references to the GDPR allow for corresponding argumenta ex contrario and thus create more confusion than clarity. To avoid this ambiguity and ensure effective implementation of privacy measures in practice, the legislator ultimately has two options: Either the legislator may specifically clarify the application of the data protection by design approach and other related provisions (in particular the processing principles, data subjects' rights and certification mechanisms) in the ePrivacy Regulation. Or, taking on a more fundamental approach, the legislator may clarify, firstly, in Art. 1 sect. 3 that "insofar as the Regulation does not provide for more specific rules, the provisions of the GDPR shall apply". Secondly, the legislator has then to clarify in the specifying provisions which GDPR provisions they refer to and to what extent (e.g., restriction of the legal basis or of purpose compatibility); in this way, the legislator can avoid unclear specifications leading to the exclusion of GDPR standards that the legislator probably did not intend to exclude.

In any case, applying the data protection by design approach to the ePrivacy Regulation means that pointless cookie banners may soon be history. If so, legislators would not have to dictate what information or control architectures should look like from a user's perspective. In addition, the rapid pace of development in the communications sector would otherwise prove extremely challenging for legislators unless a data protection by design approach is applied to the ePrivacy Regulation. The legislator can certainly make individual specifications, as is sensibly done in Article 4a of the current draft of the ePrivacy Regulation. However, the legislator should be careful not to make too



Drafting laws in a more effective way by adding methods of user-centred design

many specifications. Those specifications quickly turn obsolete or ineffectual in light of rapid advancements within the communications sector. Since data protection by design requires data controllers to implement protection **effectively** by taking the **state of the art** into account, the approach offers a two-fold advantage: Legislators provide adequate protections for data subjects while leaving the path open to build upon existing protection measures as the communication sector evolves.

This leads us to the most fundamental aspect of our criticism: How can the legislator design laws that more effectively address user needs? How can the legislator avoid ambiguities in laws that jeopardize the effective implementation of protection measures in practice? In our opinion, the legislator can achieve this goal by expanding one's legislative methods. While legislation should still draw from the legal considerations involved in the legislative information process, we suggest that this process would benefit considerably if supplemented with empirical studies and design methods such as those presented in this paper. Accordingly, the legislator could test which regulations produce which effects in practice, thereby increasing the effectiveness and the rationality of laws.[16] In conclusion, we argue for more evidence-based lawmaking through design.

16 Wolfgang Hoffmann-Riem and Saskia Fritzsche, 'Innovationsverantwortung – Zur Einleitung' in Hoffmann-Riem and Martin Eifert (eds), Innovation und Recht III – Innovationsverantwortung (Duncker & Humblot 2009) 39.

References

Art. 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 00569/13/EN WP 203

Bauer JM, Bergstrøm R and Foss-Madsen R, 'Are You Sure, You Want a Cookie? – The Effects of Choice Architecture on Users' Decisions about Sharing Private Online Data' (2021) 120 Computers in Human Behavior 106729

Baumgartner U and Gausling T, 'Datenschutz Durch Technikgestaltung Und Datenschutzfreundliche Voreinstellungen' (2017) Zeitschrift für Datenschutz 308

Choi H, Park J and Jung Y, 'The Role of Privacy Fatigue in Online Privacy Behavior' (2018) 81 Computers in Human Behavior 42

CNIL, 'Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux cookies et autres traceurs' - <https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf> accessed 18 June 2021

Council of the EU, 'Confidentiality of Electronic Communications: Council Agrees Its Position on EPrivacy Rules' <https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/> accessed 22 March 2021

Digital Rights vs Ireland (2014) ECJ C-293/12 and C-594/12

EDPB 'Guidelines on Transparency under Regulation 2016/679' (2017) 17/EN WP260 rev.01

EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, Adopted on 20 October 2020'

Hoffmann-Riem W and Fritzsche S, 'Innovationsverantwortung – Zur Einleitung' in Hoffmann-Riem and Martin Eifert (eds), Innovation und Recht III – Innovationsverantwortung (Duncker & Humblot 2009)

Omer T and Poloentsky J, 'A Theory of Creepy: Technology, Privacy and Shifting Social Norms' (2013) Yale Journal of Law and Technology

Sunstein CR, 'Choosing Not to Choose' (2014) Harvard Public Law Working Paper <https://papers.ssrn.com/abstract=2377364> accessed 5 May 2021

Verbraucherzentrale Bundesverband eV vs Planet49 GmbH (2019) ECJ C-673/17

von Grafenstein M, Jakobi T and Stevens G, 'Effective Data Protection by Design through Interdisciplinary Research Methods - The Example of Effective Purpose Specification by Applying User-Centered UX-Design Methods' (in review) CLSR

von Grafenstein M, '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 G González-Fuster, R van Brakel and P De Hert (eds), Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Edward Elgar Publishing (Edward Elgar Publishing 2019)

von Grafenstein M, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II: Controlling Risks through (Not To) Article 8 ECFR against the Other Fundamental Rights (Esp. by the Principle of Purpose Limitation)' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3840116 <https://papers.ssrn.com/abstract=3840116> accessed 19 June 2021