noyb

European Center
for Digital Rights

Consent Banner Report

Overview of EU and national guidelines on dark patterns

noyb.eu

Table of Contents

Disclaimer: This report is meant to provide an overview of the legal assessment and criteria of different data protection authorities as of **November 2023**. It was drawn up to the best of our knowledge, however it is based on the experience of noyb and may therefore not be a comprehensive assessment of each Data Protection Authority's stance. Automated translation tools were used for translating certain languages.

1. Background

noyb - European Centre for Digital Rights is an Austrian non-for-profit working in the field of privacy and data protection law. In 2021 *noyb* initiated a project investigating the proliferation of illegal consent banners which are designed to seek consent for setting of cookies on website visitors' terminal devices.

Cookies are small files which are used by websites to, among other things, save browsing information between website visits, allowing websites to remember your device and browsing preferences. Consent banners are used on websites to inform users visually about cookies and similar technologies and, usually, to request consent for the setting of cookies.

The ubiquity of consent banners across the web has led to observations of "consent banner fatigue", whereby users become tired of repetitive and inconvenient consent requests and this leaves them more susceptible to being pressured into just giving their so-called 'consent' every time. The initial investigation conducted by *noyb* revealed the extremely common-placed practice of installing dark patterns on consent banners. The term dark pattern describes deceptive design and presentation practices used to dissuade users from e.g. rejecting cookies. It was found that even very small design changes can have a significant impact on users, making it overly complicated to reject cookies, or even leading users to believe that consent is the only available option in order to access a website. After checking the web for illegal consent banners in March 2021, *noyb* subsequently filed over 600 complaints against the most visited pages containing illegal consent banners.

Regarding the legal basis for this mass complaint project, according to Article 5(3) of the ePrivacy Directive, consent is required for the "storage of information or access to information already stored in the terminal equipment of a subscriber or user". While the General Data Protection Regulation (hereinafter "GDPR") does not provide for a specific regulation on the setting of cookies, it applies to the processing of the personal data processed through cookies. The storage and access to the information is therefore regulated in the ePrivacy Directive.

However, consent must be obtained according to the standards of the GDPR, which is also provided for in Article 2(f) of the ePrivacy Directive. Therefore, in order for consent to be valid, it must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes". It was *noyb*'s view that consent obtained from consent banners involving dark patterns, could not be considered valid according to these requirements.

A mass complaint project was necessary to, among other aims, establish some of the precise practices which violate data protection law. In particular, the complaints focused on eight widely-observed practices: no reject button on the first layer (type A); pre-ticked boxes (type B); deceptive link design (type C); deceptive button co-

lours (type D); deceptive button contrast (type E); "legitimate interest" claimed (Type H); Inaccurately classified "essential cookies" (type I); and not as easy to withdraw as to give consent (type K).

As various complaints were filed with data protection authorities (DPAs) across the EEA, a Task Force was set up by the European Data Protection Board (EDPB) to "to coordinate the response to complaints". [1] In January 2023, the taskforce published a report titled "Report of the work Undertaken by the Cookie Banner Taskforce" which offered their opinion and recommendations regarding each of the violations outlined above. [2]

It is important to note, firstly, that the initial pages of the report contain a disclaimer, clearly stating that the task force findings are only **minimum thresholds** for consent banners, and that national DPAs are able to adopt higher standards. However, it appears that, for a number of the practices contained in the report, the recommendations of the EDPB are more general, lenient, or vague than those contained in the guidelines adopted by individual DPAs. In particular, while many national authorities adopt strict rules with specific requirements and examples, the EDPB report often endorses a "case-by-case" approach or recommends a low threshold, or one with room for interpretation.

The purpose of this report is to offer a comprehensive account of the EDPB taskforce's report findings for each violation, compared with the positions taken by national DPAs in guidance documents. It is hoped that this will initiate further discussion regarding the guidelines adopted concerning deceptive practices, and how these can be developed in the future to facilitate valid consent and ensure effective compliance with the law.

The Report will address each practice in turn, outlining some relevant issues, the position of the EDPB taskforce, and the guidelines published by the national DPAs. Where available, information about actual DPA decisions will be added. Thereafter, the report will offer an overview of all of the national DPA guidelines discussed in this report, in order to provide sources, context and further information. The final section of the report will outline some other relevant EDPB and WP29 guidelines for further research.

[1] https://edpb.europa.eu/news/news/2021/edpb-establishes-cookie-banner-taskforce_en
[2] https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en

2. List of National DPA Guidelines

This section provides a list with some guidelines of SAs and national ePrivacy Regulators.

2.1. Austria (DSB)

Guidelines

- Updated: "FAQs about cookies and data protection" (3 May 2023)

2.2. Belgium (GBA/APD)

Guidelines

- "Cookies and other tracers" (20 October 2023)

Additional Information

The DPA published cookie guidelines on 9 April 2020. On 20th October 2023, the DPA updated its cookie checklist and added new information under the dossier "cookies" on its website.

2.3. Czech Republic (UOOU)

Guidelines

- "Cookies" (date unconfirmed)

2.4. Denmark (Datatilsynet)

Guidelines

- Datatilsynet "Processing of personal data of website visitors" (February 2020)

Additional Information

There are two laws for cookies in Denmark:

- The Danish Cookie Law (Cookiebekendtgørelsen); and,
- The General Data Protection Regulation of the EU - GDPR (and the Data Protection Act of Denmark).

Authorities which have published guidelines:

- Danish DPA (Datatilsynet)
- Danish Business Authority
- Danish Business Authority and Danish Council for Digital Security (joint guidance)

2.5. Finland (Traficom – Transport and Communications Agency)

Guidelines

- "Traficom Cookie Guidelines" (November 2022)

Additional Information

The Office of the Data Protection Ombudsman is the national supervisory authority in Finland. Traficom (the Finnish Transport and Communications Agency) is the authority responsible for monitoring and ensuring the confidentiality of electronic communications. It is also the competent authority on cookie regulation and supervision of the use of cookies. In April 2020, Traficom held it was possible to give consent through browser settings. Thereafter, in May 2021, Traficom changed its cookie guidelines to reflect the decisions of the Data Protection Ombudsman. The guidelines were later updated, on 11 November 2022.

2.6. France (CNIL)

Guidelines

- "Cookies and other tracers" guidelines (17 September 2020, published 1 October 2020)
- "Cookies and other tracers" recommendations (17 September 2020, Published 1 October 2020)

Press Releases

- 1 October 2020, Cookies and tracers: what does the law say?
- 1 October 2020, Cookies and other tracers: the CNIL publishes amending guidelines and its recommendation

2.7. Germany (DSK)

Guidelines

- "Guidance from the Supervisory Authorities for Telemedia providers" (Version 1.1 December 2022)

Additional Information

The Federal Act on the Regulation of Data Protection and Privacy in Telecommunications and Telemedia (TTDSG) entered into force on 1 December 2021. On 22 December 2021, the DSK issued its Guidance for Providers of Telemedia Services, which was primarily concerned with the "cookie provision" of this Act. The latter was updated and Version 1.1 was published in December 2022.

2.8. Greece (HDPA)

Guidelines

- "Recommendations for compliance of data controllers with specific electronic communications legislation" (February 2020)

2.9. Ireland (DPC)

Guidelines

- "Guidance on Cookies and other Tracking Technologies" (April 2020) (see also: press release)

Additional Information

In April 2020, following a "cookie sweep survey", the DPC issued a guidance note on the use of cookies.

2.10. Italy (Garante)

Guidelines

- "Guidelines on the use of cookies and other tracking tools" (10 June 2021)

Additional information

The Garante originally published a resolution, on 8 May 2014, about streamlined procedures for information notices and gaining consent for the use of cookies. On 10 June 2021, they published updated guidelines.

2.11. Latvia (DVI)

Guidelines

- Latvian DPA Cookie Guidelines

Additional Information

In March 2022, the Latvian DPA published Cookie Guidelines and a model cookie policy.

2.12. Luxembourg (CNPD)

Guidelines

- "Guidelines on Cookies and Other Tracking Devices" (January 2022)
- The CNPD also issued a "Practical guide on cookies and other tracking devices"

2.13. Netherlands (AP)

Guidelines

- "More information about cookies"

Additonal Information

Following a survey of 175 websites which found 50% to be non-compliant, the Dutch DPA, in December 2019, published a press release with cookie consent guidelines.

2.14. Portugal (CNPD)

Information

In July 2021, the Portuguese DPA issued a note stating they plan to issue guidelines on the use of cookies. However, in its annual report of 2022, the DPA stated that since the EDPB Taskforce Report was published in 2023, the DPA considered it reasonable to postpone the adoption of their own guidelines on the use of cookies in order to adapt them to the content of the Report, notwithstanding its non-binding nature (see CNPD annual report of 2022).

2.15. Spain (AEPD)

Guidelines

- "Guide to the use of cookies"
- The new Guidelines recently adopted by the AEPD entail new criteria for the assessment of consent banners violations, which resemble more the approach of the EDPB. One of the main changes in the updated version of the Guidelines is the need to show an accept and reject option on the same layer of the banner, so that it is as straightforward to grant as to withdraw one's consent. However, the AEPD specified that these Guidelines **will only be applicable from 11th January 2024 onwards**, at the latest, hence past cases were and will still be assessed on the basis of the previous guidelines.

Additional Information

The Spanish DPA's cookie guidelines were originally published in November 2019, then updated on 28 July 2020, to reflect the changes made to the EDPB consent guidelines. On 11 July 2023, the AEPD further updated the Guidelines to reflect the changes made to the EDPB "Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them". Press Release (11 July 2023)

Other Countries

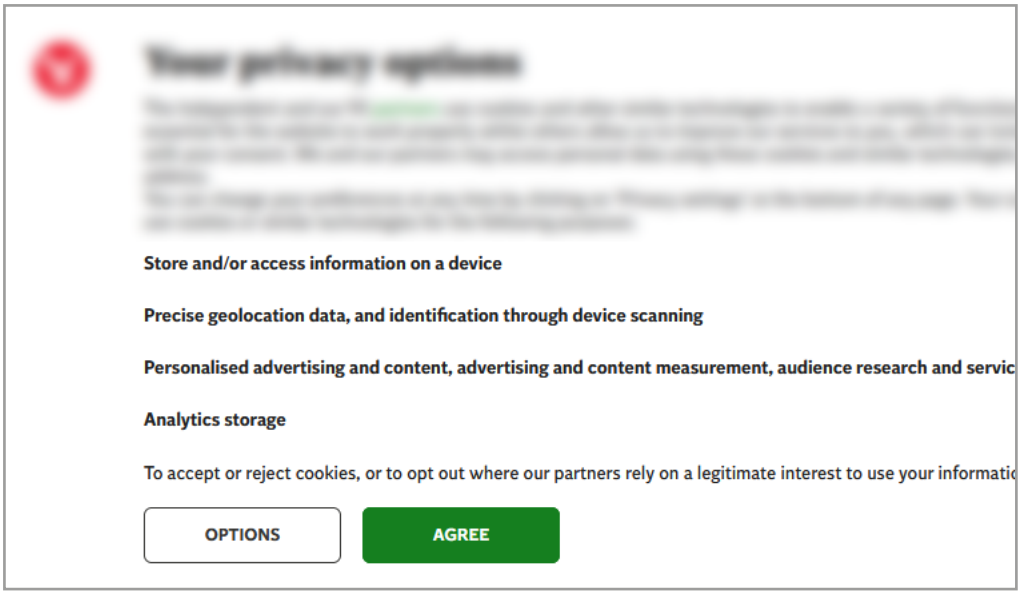
Other guidelines are not discussed in this report.

3. Issues, EDPB Report, National DPA Guidelines and National DPA Decisions

3.1. Issue 1: No Reject Button on the First Layer

Issue

No option to 'reject' consent is available on the first layer of the consent banner. This impacts on the behaviour of users: According to industry numbers, only 2,18% of data subjects visit the second layer. Also, rejecting consent requires at least twice as many steps as consenting.



EDPB Report on the Work Undertaken by the Cookie Banner Taskforce

"8. When authorities were asked whether they would consider that a banner which does not provide for accept and refuse/reject/not consent options on any layer with a consent button is an infringement of the ePrivacy Directive, **a vast majority of authorities considered that the absence of refuse/reject/not consent options on any layer with a consent button of the cookie consent banner is not in line with the requirements for a valid consent and thus constitutes an infringement**. Few authorities considered that they cannot retain an infringement in this case as article 5(3) of the ePrivacy Directive does not explicitly mention a "reject option" to the deposit of cookies."

National DPA Guidelines

Austria (DSB)

- "Not giving consent is as easy as giving consent: Not giving consent (or continuing to surf without consent) must be as easy as giving consent. In other words: Not giving consent **should not require more** interactions with the consent banner than giving consent. It cannot be required of the data subject that they can only make the decision not to give their consent on a button at a second or third level."

Belgium (GBA/APD)

- Users **must be able to accept or refuse**, for each application and each website, the deposit of cookies **without constraint, pressure or influence**. This requirement implies, in particular, that users cannot be refused certain services or benefits on the grounds that they have not consented to the use of "non-functional" cookies. A person who refuses a cookie requiring consent must be able to continue to benefit from the service, such as access to a website. **"Cookie walls" are therefore not authorised** because they do not allow valid consent to be obtained under the GDPR.

- The design of the consent banner can also have the effect of compromising the free nature of consent. This is the case, for example, when an "accept all cookies" button (or similar) without providing a "refuse all non-strictly necessary cookies" button (or similar) at the same "level".

Czech Republic (UOOU)

- "In the so-called consent banner, **a reject button for non-essential cookies needs to be placed** in a way so that potential consent is given without coercion and the visitor to the website is not influenced in their choice (it should be as easy to not give consent as to give it). The consent banner layout that meets this condition is where the accept button and reject button for non-essential cookies are placed in the same layer of the consent banner, and an example of good practice is where the reject button for non-essential cookies is placed in the first layer of the consent banner (in the same layer and in a comparable visual design as the accept button)."

- "In order for the data subject to have a free choice, **refusing consent must be as simple as giving it**, which is achieved by placing the accept and reject non-essential cookies buttons in the same layer of the consent banner."

Denmark (Datatilsynet)

- "A mechanism or solution for obtaining consent where the option to refrain from giving consent to the processing of personal data does not have **the same communication effect** as the option to give consent would not be lawful, as the data subject is indirectly pushed in the direction of giving consent."

- "In the opinion of the Danish Data Protection Agency, this is contrary to the fundamental principle of transparency."

Finland (Traficom – Transport and Communications Agency)

- "In addition, **refusing to give consent must be as uncomplicated** as granting the consent. In the case of cookies this means that granting consent for non-essential cookies must not be any less complicated than refusing consent. Example: If an "Accept or allow all" selection is offered for granting consent for all non-essential cookies on the top level of the consent mechanism, a similar option to continue using the service only with essential cookies or to refuse consent for non-essential cookies should also be offered. In this case, granting and refusing to grant consent are equally easy or uncomplicated."

France (CNIL – Recommendations)

- "…the Commission **strongly recommends that the mechanism for expressing a refusal to consent to reading and/or writing operations be accessible on the same screen and with the same ease as the mechanism for expressing consent**. Indeed, it considers that consent interfaces that require a single click to consent to tracking while several actions are necessary to "set" a refusal to consent present, in most cases, the risk of biasing the choice of the user, who wishes to be able to view the site or use the application quickly."

- "For example, at the first level of information, **users may have a choice between two buttons presented at the same level and in the same format, with 'accept all' and 'reject all', or 'authorize' and 'do not authorize', or 'consent' and 'no consent' written on them respectively,** The Commission considers that this modality is a simple and clear way to allow the user to express his refusal as easily as his consent."

Germany (DSK)

- "In cases where it is not possible to remain inactive because a consent banner blocks access to some or all of the content of the telemedia offer, **end-users must at least be able to express their refusal without additional clicks** (compared to consent)."

- "It is crucial that the option to reject cookies is perceived as such by users. It is **not sufficient**, for example, that the option to reject is presented **outside of**

the banner, on the website or if this is shown in the body text of the banner without being clearly visually emphasised or highlighted, while the option to consent appears prominently as a button outside the body text. Even an identical button, which is however **only visible after scrolling** through the text of the banner, while the option to give consent is placed at the beginning of the banner **cannot be easily recognised as an equivalent alternative.**"

- "If a button for refusing consent is offered next to the button for consent, the **labelling must be unambiguous** so that users know that they are not giving consent. This can be illustrated by a short and concise labelling. A 'settings or reject' button, which leads to a further layer of the banner, is not sufficient in this regard".

Greece (HDPA)

- "The user should be able, with the **same number of actions ("clicks")** and from the same level, either to accept the use of the trackers (those for which consent is required) or to reject it, either all or each category separately."

Ireland (DPC)

- "If you use a consent banner or pop-up, **you must not use an interface that 'nudges' a user** into accepting cookies over rejecting them. Therefore, if you use a button on the banner with an 'accept' option, **you must give equal prominence** to an option which allows the user to 'reject' cookies, or to one which allows them to manage cookies and brings them to another layer of information in order to allow them do that, by cookie type and purpose."

- "You **must include a link or a means of accessing further information** about your use of cookies and the third parties to whom data will be transferred when the user is prompted to accept the use of cookies."

Italy (Garante)

- "If the user chooses, as he or she is fully entitled to do, to keep the default settings and therefore not to give his or her consent to the storing of cookies or the use of other tracking techniques, **that user should therefore simply close the banner** by clicking on the command that is usually meant to enable this action – i.e., the 'X' that is normally positioned according to well-received practice at the top right end of the banner area - without having to access other ad-hoc areas or pages. The command in question will have to be **as visible as any other commands or buttons** that may be used to flag other choices available to the users, which will be detailed below. In other words, the mechanism to enable continued browsing without giving any consent will have to be **as user-friendly and accessible** as the one in place for giving one's consent."

Luxembourg (CNPD)

- "...the GDPR implies that consent must be freely given. In line with this spirit, the CNPD strongly recommends that the **same possibilities for giving consent as for refusing it** should be offered."

- "This means that, if it takes several operations (number of clicks or other) to accept a specific purpose, it should not take a greater number of operations to reject it. Similarly, if an "I accept all" button is present on the first layer, **a similar "I refuse all"** button should also be present."

- "Indeed, the CNPD considers that if it is possible to consent with a single click, whereas several clicks are necessary to express a refusal to consent, there is a risk of biasing the user's choice, as the latter generally wishes to access the website as quickly as possible."

Netherlands (AP)

- "If you offer your visitors an information sidebar with a **clear choice between 'yes' and 'no',** you at least meet the choice requirement for unambiguous consent. Provided, of course, that you do not place any cookies before the visitor has made a choice."

Spain (AEPD)

- "The first layer, which for clarity may be identified by a commonly used term (e.g. "cookies"), will include the following information:
  (e) How the user can **accept, configure and reject** the use of cookies."

- "In connection with point e) above of this first layer of information, this should contain:
  - (a) A **button or equivalent** mechanism, easily visible, with the words 'accept cookies', 'accept', 'consent' or similar text, **to consent to the use of all cookies**
  - (b) A **button or equivalent** mechanism, similar to the above (if an 'accept' button is used, a 'reject' button should be used), with the words "Reject cookies", 'reject' or similar text, **to refuse the use of cookies** (except for those that are exempted from the obligation to obtain informed consent)."

National DPA Decisions

Austria (DSB)

- With respect to this issue, the DSB takes the same stance as the EDPB and its own Guidelines. In its decisions, the DSB repeatedly states that a consent banner can only be valid if the user has an option to close the banner without accepting cookies already on the first layer, next to the 'accept' option. This can be done either by including a 'reject' or a "close banner without accepting" button next to the accept option, so that they are equally visible. It is worth noting that the DSB's decisions this issue are in contradiction with the CNIL Recommendations, whereby a small 'reject' option in the top corner of a consent banner may be acceptable. The Austrian DPA did not considered this an equivalent reject option.

Bavaria (BayLDA)

- According to the BayLDA, an option to reject consent is generally to be made available in the first layer of a consent banner. In case C037-12500, the BayLDA considered that a link named "continue without accepting", at the top of the banner, while the accept option is designed as a button in a more central position, to be a clear enough alternative to reject one's consent on the first layer of the banner. Interestingly, this contradicts the DSB view that a "continue without accepting" option shall be deemed lawful, only if placed next to the accept option, so that they are equally visible.

Berlin (BInBDI)

- In its decisions, the BInBDI takes the stance, in accordance with the German DSK, that a valid consent is generally not given if an 'accept' option but no 'reject' option exists as this leads to an 'effect and information deficit'.

Hessen (HBDI)

- The HBDI reiterates in its decisions that consent banners are only allowed insofar as they are based on the user's consent and such consent respects the requirements of Articles 4(11), 6(1)(a) and 7 GDPR. In case C037-10408, the HBDI was satisfied with the controller's adaptation of their consent banner so that it showed an option to reject consent on the first layer of the banner equivalent in form, colour and size to the accept option.

Luxembourg (CNPD)

- The CNPD held, in case C037-10706, that it was satisfied with the website operator's adaptation of the consent banner so that it included both accept and reject options on the first layer of the banner.

Nordrhein Westfalen, NRW (LDI)

- Upon checking the consent banners displayed on the websites against which complaints were filed, the LDI was satisfied with a reject option on the first layer of the banner, designed in such a way that it is equivalent to the accept option "in the user's eyes".

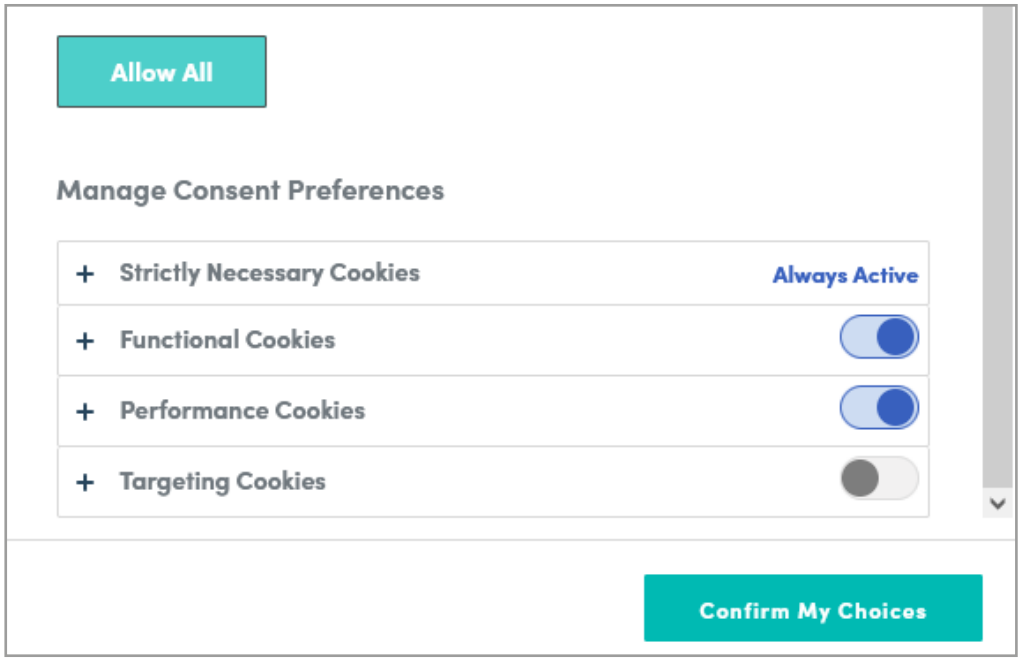
Spain (AEPD)

- The AEPD in case C037-222, followed its old Guidelines of 2020 by accepting also consent banners that do not show a 'reject' option on the first layer but only give an option to reject consent in a second layer of the banner. This is not in line with the EDPB Taskforce Report on this issue. Even though the AEPD adopted a new set of Guidelines that require that a reject option is displayed on the first layer of the banner, these only applied from January 2024.

3.2. Issue 2: Pre-Ticked Boxes

Issue

Some consent banners contain pre-ticked boxes. Users would have to untick each box in order to reject consent. This requires additional effort compared to just consenting with one click and does not lead to valid consent according to the CJEU (para. 55 of Judgment in the case C-673/17 – Planet 49), the EDPB (para. 79 of Guidelines 05/2020 on Consent) and is stated in the GDPR itself (Recital 32).



EDPB Report on the Work Undertaken by the Cookie Banner Taskforce

"9. It appears that several controllers provide users with several options (typically, representing each category of cookies the controller wishes to store) with pre-ticked boxes on the second layer of the consent banner (after the user clicked on the 'settings' button of the first layer)."

"10. The taskforce members confirmed that **pre-ticked boxes to opt-in do not lead to valid consent** as referred to either in the GDPR (see in particular recital 32 "Silence, pre-ticked boxes or inactivity should not therefore constitute consent.") or in Article 5(3) of the ePrivacy Directive."

National DPA Guidelines

Austria (DSB)

- "Privacy by default: the data subject must proactively choose to give consent. Default settings or **pre-checked boxes in the consent banner are not permitted**"

Belgium (GBA/APD)

- "Consent is **not valid** if it is collected by means of a **box ticked by default** that the user must untick to refuse to give consent."
- "Visitors must be able to give their consent, at the very least, for each type of cookie."

Czech Republic (UOOU)

- "**Pre-ticked boxes cannot be considered as consent** in accordance with the General Data Protection Regulation, which follows from Recital 32. The same conclusion was reached by the CJEU in the case of Planet49 GmbH (C 673/17)."

Denmark (Datatilsynet)

- "In contrast, passivity, silence or the continued use of a website **cannot be considered as an active opt-in** and therefore cannot constitute valid consent. The same applies to **pre-ticked opt-in boxes,** "on" sliders, etc. that require an action by the data subject to prevent consent."

Finland (Traficom – Transport and Communications Agency)

- "Cookie banners **may not include pre-ticked boxes** or slide switches in the "ON" position for non-essential cookies. Therefore, non-essential cookies may not be turned on by the service or the website by default, and the user must explicitly agree to their use by clicking on them (opt-in)."
- "Consent must be an active expression indicating the data subject's wish. Silence, **pre-ticked boxes** or inactivity should therefore **not constitute as consent.**"

France (CNIL)

- "…any inaction or action by users other than a positive act of consent should be interpreted as a refusal to consent."
- "The Commission considers that a request for consent by means of checkboxes, **unchecked by default**, is easily understandable by users. The controller may also use sliders, deactivated by default."

Germany (DSK)

- "…requires an 'unequivocal expression of will in the form of a declaration' or another unambiguous affirmative act by which users indicate that they expressly consent to accessing and retrieving information. Positive action by the end user is therefore always required."

- "Silence, **already ticked boxes** or inactivity on the part of the user, on the other hand, **cannot constitute consent.** Opt-out procedures are therefore always unsuitable to establish effective consent."

Greece (HDPA)

- "Consent requires clear affirmative action. **Pre-filled boxes,** simply continuing to navigate or scrolling **are not acceptable forms of consent.**"

Ireland (DPC)

- "The user's consent must be specific to each purpose for which you are processing their data, it must be freely given and unambiguous and it requires a clear, affirmative action on the part of the user. **Silence or inaction** by the user **cannot constitute their consent** to any processing of their data."

Italy (Garante)

- "Silence, **pre-ticked boxes** or inactivity should **not** therefore constitute consent."

Luxembourg (CNPD)

- "…consent must be manifested by a clear positive action by the person who has been informed in advance of the consequences of his or her choice. The manifestation of will can be expressed, for example, by ticking a box or activating a button by sliding."

- "However, the following cases **cannot be considered as a positive act** of the user, and therefore do not constitute unambiguous consent… **not unchecking a pre-checked box.**"

Netherlands (AP)

- "A **pre-ticked box with 'yes'** when the user is asked for consent is therefore **not allowed.** Silence, inactivity or scrolling down or variations on 'you agree if you continue on this website' are also not allowed."

Spain (AEPD)

- "...it should be remembered that **in no case are pre-ticked boxes** in favour of accepting cookies **admissible in order to obtain a valid consent.**"

National DPA Decisions

Disclaimer: As regards this issue, none of the complaints filed by noyb for which a decision is available contain claims referring to this issue. For this reason, no decisions are cited in this section.

3.3. Issue 3: Deceptive Link Design

Issue

The only clearly interactive option is the 'accept all' button as the 'reject' option simply appears as a link. Data subjects are, in this case, led to believe that there is no other option than 'accept all', especially when taking only a short look at the banner.

This practice deceives and misleads users as no genuine display of choices is available. This is at odds with the idea of 'freely given', 'informed' and 'unambiguous' consent.

EDPB Report on the Work Undertaken by the Cookie Banner Taskforce

"12. The taskforce members agreed that in any case, there should be a clear indication on what the banner is about, on the purpose of the consent being sought and on how to consent to cookies."

"13. The members agreed that for the consent to be valid, the user should be able to understand what they consent to and how to do so. In order for a valid consent to be freely given, the taskforce members agreed that in any case **a website owner must not design consent banners in a way that gives users the impression that they have to give a consent to access the website content, nor that clearly pushes the user to give consent** (one way could be on the contrary to allow the continuation of the navigation without cookies from the first level in particular for example)."

"14. The taskforce members agreed that the following examples do not lead to valid consents (non-exhaustive list):

- **the only alternative action offered** (other than granting consent) consists of **a link** behind wording such as 'refuse' or 'continue without accepting' **embedded in a paragraph of text** in the consent banner, **in the absence of sufficient visual support** to draw an average user's attention to this alternative action;

- **the only alternative action offered** (other than granting consent) consists of **a link** behind wording such as 'refuse' or 'continue without accepting' **placed outside the consent banner** where the buttons to accept cookies are presented, **in the absence of sufficient visual support** to draw the users' attention to this alternative action outside the frame;"

National DPA Guidelines

Austria (DSB)

- **"Not giving consent** (or continuing to surf without consent) **must be as easy as giving consent.** In other words: Not giving consent should not require more interactions with the consent banner than giving consent. It cannot be required of the data subject that they can only make the decision not to give their consent on a button at a second or third level."

- "No unfair practices: The data subject **must not be directly or subtly pressurised into giving consent** (no "nudging"). It is **unlawful to design or position the button** for **not giving consent** (or for continuing to surf without consent) in such a way that this button **is less prominent** than the button for giving consent."

Czech Republic (UOOU)

- "In the so-called consent banner, **a reject button for non-essential cookies needs to be placed** in a way so that potential consent is given without coercion and the visitor to the website is not influenced in their choice (it should be as easy to not give consent as to give it). The consent banner layout that meets this condition is where the accept button and reject button for non-essential cookies are placed in the same layer of the consent banner, and an example of good practice is where the reject button for non-essential cookies is placed in the first layer of the consent banner (in the same layer and in a comparable visual design as the accept button)."

- "In order for the data subject to have a free choice, **refusing consent must be as**

simple as giving it, which is achieved by placing the accept and reject non-essential cookies buttons in the same layer of the consent banner."

Denmark (Datatilsynet)

- "A mechanism or solution for obtaining consent where the option to refrain from giving consent to the processing of personal data does not have the **same communication effect** as the option to give consent **would not be lawful,** as the data subject is indirectly pushed in the direction of giving consent."

- "In the opinion of the Danish Data Protection Agency, this is contrary to the fundamental principle of transparency."

Finland (Traficom – Transport and Communications Agency)

- "In addition, refusing to give consent must be **as uncomplicated** as granting the consent. In the case of cookies this means that granting consent for non-essential cookies must not be any less complicated than refusing consent. Example: If an "Accept or allow all" selection is offered for granting consent for all non-essential cookies on the top level of the consent mechanism, a **similar option** to continue using the service only with essential cookies or to refuse consent for non-essential cookies should also be offered. In this case, granting and refusing to grant consent are **equally easy or uncomplicated.**"

Germany (DSK)

- "If one option is presented precisely and produces an immediate effect (e.g. an 'accept all' button), while the **other option is kept nebulous** and does not allow the true contrary intention to be expressed with the same effort, there is an **effect and information deficit.** Such a deficit is likely to lead end-users to make their decision not according to the clear will, but only according to which option clearly ends the consent request faster. If users are not offered equivalent options to give or refuse consent, **the requirements for effective consent are regularly not met.**"

- "The option to reject consent must be clearly presented as an equivalent alternative to the option to give consent. This is assumed, for instance, if next to an 'accept' button there is a similar "continue without accepting" button, in particular in terms of size, colour, contrast and typeface."

- "It is crucial that the option to reject cookies is perceived as such by users. It is **not sufficient**, for example, that **the option to reject is presented outside of the banner**, on the website or if this is shown in the body text of the banner **without being clearly visually emphasised or highlighted**, while the option to consent appears prominently as a button outside the body text. Even an identical button, which is however only visible after scrolling through the text of the

banner, while the option to give consent is placed at the beginning of the banner cannot be easily recognised as an equivalent alternative."

Greece (HDPA)

- "The user should be able, with the **same number of actions** ("clicks") and from the same level, either to accept the use of the trackers (those for which consent is required) or to reject it, either all or each category separately."

Ireland (DPC)

- "If you use a consent banner or pop-up, you must **not use an interface that 'nudges'** a user into accepting cookies over rejecting them. Therefore, if you use a button on the banner with an 'accept' option, you must give **equal prominence to an option which allows the user to 'reject' cookies**, or to one which allows them to manage cookies and brings them to another layer of information in order to allow them do that, by cookie type and purpose."

- "You must include a link or a means of accessing further information about your use of cookies and the third parties to whom data will be transferred when the user is prompted to accept the use of cookies."

Italy (Garante)

- "If the user chooses, as he or she is fully entitled to do, to keep the default settings and therefore not to give his or her consent to the storing of cookies or the use of other tracking techniques, **that user should therefore simply close the banner** by clicking on the command that is usually meant to enable this action – i.e., the 'X' that is normally positioned according to well-received practice at the top right end of the banner area - without having to access other ad-hoc areas or pages. The command in question will have to be **as visible as any other commands or buttons** that may be used to flag other choices available to the users, which will be detailed below. In other words, the mechanism to enable continued browsing without giving any consent will have to be as user-friendly and accessible as the one in place for giving one's consent."

Luxembourg (CNPD)

- "...the GDPR implies that consent must be freely given. In line with this spirit, the CNPD strongly recommends that the **same possibilities for giving consent as for refusing it** should be offered."

- "This means that, if it takes several operations (number of clicks or other) to accept a specific purpose, it should not take a greater number of operations to reject it. Similarly, if an 'I accept all' button is present on the first layer, **a similar 'I refuse all'** button should also be present."

- "Consent can only be valid if users are able to exercise their choice genuinely and freely, without being forced in any way to accept the use of cookies."

- "The CNPD recalls that data controllers **must avoid misleading – consciously or not – users** when seeking their consent."

- "It therefore recommends that the operators of websites or applications present, in an **identical manner,** the different choices available to the user regarding the acceptance of cookies."

- "In particular, the CNPD recommends avoiding the use of some or all of the following deceptive design practices, which are designed to trick the user and are part of the "dark patterns" phenomenon: **Different forms of 'consent buttons' (e.g. the use of a large 'I agree' button, whereas the 'I decline' button is presented only as a small hyperlink)"**

Netherlands (AP)

- "If you offer your visitors an information sidebar with a **clear choice between 'yes' and 'no',** you at least meet the choice requirement for unambiguous consent. Provided, of course, that you do not place any cookies before the visitor has made a choice."

Spain (AEPD)

- The guidelines provide two different examples of valid consent banners
  - Example 1 – 'accept', 'reject' and 'configure'" buttons
  - Example 2 – 'yes' and 'no' buttons and a 'configure without accepting' link

National DPA Decisions:

Austria (DSB)

- In its decisions, the DSB takes the stance that both the consent and reject options must be equally visible. This includes the criterion that the alternative used to reject cookies is not presented in the form of a link if this is not the case for the consent option.

Bavaria (BayLDA)

- The BayLDA was satisfied with the possibility of rejecting cookies displayed as a link, while the accept option is designed as a button. It considered this practi-

ce would still be acceptable since it can be perceived as an equally valid reject option by the user. Concretely, the BayLDA held in case C037-12500, that a link named 'continue without accepting', at the top of the banner constitutes a clear enough alternative to reject one's consent even where the accept option is designed as a button. This is in line with the generic Guidelines of the DSK but contradicts the Austrian DSB's decisions on this specific design choice.

Berlin (BInBDI)

- The BInBDI does not mention the link design feature specifically in its decisions, but makes an assessment of the legality of the consent banner with respect to violation types C, D, E together. The BInBDI is of the opinion that notwithstanding the design, colour and contrast choices of the presented options, it is relevant to ascertain whether there is a possibility to close a banner without accepting on the first layer and this shall be assessed on a case by case basis. In case C037-12299, the BInBDI held that the accept and reject options must have the same 'Kommunikationseffekt', that is, it must be unequivocally clear from the way in which the button is designed that this will lead to a certain effect. In the BInBDI's view this is a mere matter of perception and it is irrelevant that the accept and reject options are not identical in colour, style or contrast, since what is more important is that the user is able to recognise the options as such.

Hessen (HBDI)

- In case C037-11052, the HBDI was satisfied with the controller's adaptation of their consent banner in a manner that it displayed the reject option in the same form as the accept option, so that they could be considered as equivalent alternatives.

Spain (AEPD)

- The Spanish AEPD did not consider that the link-design of the reject option is unlawful where the accept alternative is framed as a button. Such unequal design is accepted in the AEPD Guidelines of 2020 but is not in line with the EDPB Taskforce Report on this issue. It is also not in line with the updated AEPD Guidelines which become applicable in January 2024.

3.4. Issue 4: Deceptive Button Colours

Issue
Different colours are used for the options on the consent banner. Mainly, the 'accept all' button is highlighted, which tends to indicate that it is the expected action and the 'easy way out'.

When the 'accept all' option is highlighted over other options, it violates the principles of 'fairness' and 'transparency' (Article 5(1)(a) GDPR). The wish expressed by the data subject is not 'unambiguous' (Article 4(11) GDPR) when the data subject is misled to giving consent rather than refusing it.

EDPB Report on the Work Undertaken by the Cookie Banner Taskforce
The taskforce members agreed to examine issue 4 and 5 together as the issues are linked and raise similar points of discussion.

"17. The taskforce members agreed that **a general banner standard concerning colour and/or contrast cannot be imposed on data controllers.** In order to assess the conformity of a banner, **a case-by-case verification must be carried out** in order to check that the contrast and colours used are **not obviously misleading** for the users and do not result in an unintended and, as such, invalid consent from them. As a result, it was also agreed that a case-by-case analysis would be necessary to address specific cases, although some examples of features manifestly contrary to tthe ePrivacy Directive provisions have been identified.

18. Based on concrete examples, the taskforce members took the view that **at least this practice** could be manifestly misleading for users:

- an alternative action is offered (other than granting consent) in the form of a button where the **contrast between the text and the button background is so minimal that the text is unreadable to virtually any user.**

19. While the design choices above are considered problematic, the taskforce members reiterated that each specific consent banner needs to be assessed on a case-by-case basis"

National DPA Guidelines

Austria (DSB)

- "…no unfair practices: the data subject must not be pressured into giving consent, either directly or subtly (**no "nudging"**). It is not permitted to **design or position** the button for not giving consent (or for continuing to surf without consent) in such a way that this button is less prominent than the button for giving consent."

- **"No general statement can be made about which colours** a button within a consent banner must have. The criterion for the validity of consent is, among other things, that no unfair practices are used (see question 7). It therefore depends on a case-by-case assessment."

- "If the **colour selection** means that the button for not giving consent (or for continuing to surf without consent) is less visible than the button for giving consent, this could lead to the declaration of consent being invalid."

Czech Republic (UOOU)

- "In the so-called consent banner, a reject button for non-essential cookies needs to be placed in a way so that potential consent is given without coercion and the visitor to the website is not influenced in their choice (it should be as easy to not give consent as to give it). The consent banner layout that meets this condition is where the accept button and reject button for non-essential cookies are placed in the same layer of the consent banner, and an example of good practice is where the reject button for non-essential cookies is placed in the first layer of the consent banner (in the same layer and in a **comparable visual design** as the accept button)."

- "The appearance and colour of the buttons should be chosen in such a way that the data subject has an opportunity to freely decide whether to give consent or not. For example, the 'accept' button should not be significantly larger or significantly more colourful than the 'reject' button. If the reject button were less visible or identifiable, **the data subject could miss it** and the consent given would not be considered free. At the same time, the colours of the buttons should be chosen in such a way as to respect the generally accepted meaning of these colours."

Denmark (Datatilsynet)

- "In addition, as mentioned above, in general, it must also be as easy to refrain from giving consent to the processing of one's personal data as it is to give it. This requires in particular the design of the mechanism or solution for obtaining consent, **including the visual appearance** and how the request is formulated. Overall, the option to opt-out must have the same communication effect as the option to consent."

France (CNIL)

- "In order not to mislead users, the Commission recommends that controllers ensure that choice collection interfaces **do not incorporate potentially misleading design practices** that lead users to believe that their consent is mandatory or that visually emphasise one choice over another. It is recommended that buttons and fonts be of the same size, easy to read, **and highlighted in the same way.**"

Germany (DSK)

- "In cases where end users have given their consent via a button, whether there is an unambiguous declaration of intent also depends on whether they were able to express their true will directly or could clearly see how a true will could be expressed. The assessment therefore includes how the buttons for giving consent and other options for action are **labelled and designed** and what additional information is provided."

- "The option to reject consent must be clearly presented as an equivalent alternative to the option to give consent. This is assumed, for instance, if next to an 'accept' button there is a similar "continue without accepting" button, in particular in terms of size, colour, contrast and typeface."

Greece (HDPA)

- "To ensure that the user is not biased by design choices in favour of opt-in versus opt-out, it is recommended to use buttons and font of the same size, emphasis and **colour** that provide the same ease of reading."

Ireland (DPC)

- "If you use a consent banner or pop-up, **you must not use an interface that 'nudges'** a user into accepting cookies over rejecting them."

- **"Take accessibility into account** in designing your interfaces. If you use **colour schemes** for your consent banners or your sliders and checkboxes that blend into the overall background of your site, these settings can be hard to navigate, particularly for people with vision impairments or colour blindness. While binary, colour-coded sliders or buttons may purport to signify a YES and NO option or an ON and OFF option, these colour schemes are not always accessible or self-explanatory to users who do not see colours the same way as other people. Consider testing your interface with users who have vision or reading impairments to make them as accessible as possible to all users."

Italy (Garante)

- "In order for consent to be obtained lawfully, a controller will also be required to make sure that any mechanisms for giving one's consent online other than those proposed in these Guidelines are implemented in such a way as to make the effect produced by each action unambiguous for the user as well – to the extent such action is tantamount to the provision of consent. This is intended to **limit the occurrence of so-called 'false positives',** i.e. random actions that are misinterpreted as indications of the user's informed choice."

- "...one can easily dispel possible misunderstandings in interpreting the user's actions by having regard to the **specific configuration of the buttons and colours** used by publishers - which has hitherto not been unequivocal. In that regard, it is sufficient to reiterate that - irrespective of the configuration adopted, **the colours** used for the buttons and, ultimately, the implementing methods chosen - the affirmative action the user is empowered to perform when first accessing a website must in any case be aimed at giving his or her consent (so-called 'opt-in') and may never consist in refusing such consent (so-called 'opt-out')."

Luxembourg (CNPD)

- "Consent can only be valid if users are able to exercise their choice genuinely and freely, without being forced in any way to accept the use of cookies."

- "The CNPD recalls that data controllers must avoid misleading – consciously or not – users when seeking their consent."

- "It therefore recommends that the operators of websites or applications present, in an **identical manner,** the different choices available to the user regarding the acceptance of cookies.
  - In particular, the CNPD recommends avoiding the use of some or all of the-

following deceptive design practices, which are designed to trick the user and are part of the 'dark patterns' phenomenon:

- **Different colours of the consent buttons (e.g. an 'I accept' button with a** coloured background and an "I refuse" button with a white background)"

Spain (AEPD)

- "The colour or contrast of text and buttons (or equivalent mechanisms) shall not be obviously misleading to users, in such a way as to lead to an involuntary consent. It **shall not be valid,** for example, if the option to reject cookies is a button with a text that **does not contrast sufficiently with the button's colour** and is therefore not readable."

National DPA Decisions:

Austria (DSB)

- The DSB analysed a case in which a consent banner was designed in such a way that the "OK" option is displayed on a bigger, central button in red, whereas the "reject cookies" and 'settings' options are written underneath it, in black and in smaller font size, without a button, making them less visible compared to the 'accept' option (case C037-11426). In this case, the DSB held, in line with its guidelines, that such a consent banner design is unlawful as it does not allow for an unambiguous consent to be granted according to Article 4(11) and Article 7 GDPR.

Bavaria (BayLDA)

- As opposed to the DSB's conclusion in case C037-11426, the Bavarian LDA held, with respect to an identically designed consent banner as the one considered by the DSB, that notwithstanding the clear difference in colour and prominence, the 'reject' option is still recognisable as such, hence constitutes a valid alternative (see case C037-11942)

Berlin (BInBDI)

- In case C037-12299, the BInBDI held that the accept and reject options must have the same "Kommunikationseffekt", that is, it must be unequivocally clear from the way in which the button is designed that this will lead to a certain effect. In particular, the BInBDI held that internet users are now used to seeing reject and accept options in different colours, hence this does not affect their ability to reject cookies.

Hessen (HBDI)

- In case C037-11052, the HBDI was satisfied with the controller's adaptation of their consent banner which displayed the reject option in the same colour as the accept option. The DPA considered such design to offer equivalent alternatives.

Luxembourg (CNPD)

- The CNPD held, in case C037-10706, that it was satisfied with the website operator's adaptation of the consent banner solving this issue.

3.5. Issue 5: Deceptive Button Contrast

Issue
Different contrast ratios (in relation to the background) are used for the options presented in the consent banner, highlighting the 'accept' option over other options.

When the 'accept all' option is highlighted over other options, it violates the principles of 'fairness' and 'transparency' (Article 5(1)(a) GDPR). The wish expressed by the data subject is not 'unambiguous' (Article 4(11) GDPR) when the data subject

is misled to giving consent rather than refusing it.

EDPB Report on the Work Undertaken by the Cookie Banner Taskforce
The taskforce members agreed to examine issue 4 and 5 together as the issues are linked and raise similar points of discussion.

"17. The taskforce members agreed that **a general banner standard concerning colour and/or contrast cannot be imposed on data controllers.** In order to assess the conformity of a banner, **a case-by-case verification must be carried out** in order to check that the contrast and colours used are **not obviously misleading** for the users and do not result in an unintended and, as such, invalid consent from them. As a result, it was also agreed that a case-by-case analysis would be necessary to address specific cases, although some examples of features manifestly contrary to the ePrivacy Directive provisions have been identified.

18. Based on concrete examples, the taskforce members took the view that **at least this practice could be manifestly misleading** for users:

- an alternative action is offered (other than granting consent) in the form of a button where the **contrast between the text and the button background is so minimal that the text is unreadable to virtually any user.**

19. While the design choices above are considered problematic, the taskforce members reiterated that each specific consent banner needs to be assessed on a case-by-case basis."

National DPA Guidelines

Austria (DSB)

- "...no unfair practices: the data subject must not be pressured into giving consent, either directly or subtly (**no 'nudging'**). It is not permitted to **design or position** the button for not giving consent (or for continuing to surf without consent) in such a way that this button is **less prominent** than the button for giving consent."

Czech Republic (UOOU)

- "In the so-called consent banner, a reject button for non-essential cookies needs to be placed in a way so that potential consent is given without coercion and the visitor to the website is not influenced in their choice (it should be as easy to not give consent as to give it). The consent banner layout that meets this condition is where the accept button and reject button for non-essential cookies are placed in the same layer of the consent banner, and an example of good practice is where the reject button for non-essential cookies is placed in the first layer of the consent banner (in the same layer and in a **comparable visual design** as the accept button)."

- "The appearance and colour of the buttons should be chosen in such a way that the data subject has an opportunity to freely decide whether to give consent or not. For example, the 'Accept' button **should not be significantly larger or significantly more colourful** than the 'Reject' button. If the reject button were less visible or identifiable, **the data subject could miss it** and the consent given would not be considered free. At the same time, the colours of the buttons should be chosen in such a way as to respect the generally accepted meaning of these colours."

Denmark (Datatilsynet)

- "In addition, as mentioned above, in general, it must also be as easy to refrain from giving consent to the processing of one's personal data as it is to give it. This requires in particular the design of the mechanism or solution for obtaining consent, **including the visual appearance** and how the request is formulated. Overall, the option to opt-out must have the same communication effect as the option to consent."

France (CNIL)

- "In order not to mislead users, the Commission recommends that controllers ensure that choice collection interfaces **do not incorporate potentially misleading design practices** that lead users to believe that their consent is mandatory or that visually emphasise one choice over another. It is recommended

that buttons and fonts be of the same size, **easy to read, and highlighted in the same way.**"

Germany (DSK)

- "In cases where end users have given their consent via a button, whether there is an unambiguous declaration of intent also depends on whether they were able to express their true will directly or could clearly see how a true will could be expressed. The assessment therefore includes how the buttons for giving consent and other options for action are **labelled and designed** and what additional information is provided."

- "The option to reject consent must be clearly presented as an equivalent alternative to the option to give consent. This is assumed, for instance, if next to an 'accept' button there is a similar "continue without accepting" button, in particular in terms of size, colour, contrast and typeface."

Greece (HDPA)

- "To ensure that the user is not biased by design choices in favour of opt-in versus opt-out, it is recommended to use buttons and font of the same size, **accent** and colour that provide **the same ease of reading.**"

Ireland (DPC)

- "If you use a consent banner or pop-up, **you must not use an interface that 'nudges'** a user into accepting cookies over rejecting them."

- "**Take accessibility into account** in designing your interfaces. If you use colour schemes for your consent banners or your sliders and checkboxes that **blend into the overall background** of your site, these settings can be hard to navigate, particularly for people with vision impairments or colour blindness. While binary, colour-coded sliders or buttons may purport to signify a YES and NO option or an ON and OFF option, these colour schemes are not always accessible or self-explanatory to users who do not see colours the same way as other people. Consider testing your interface with users who have vision or reading impairments to make them as accessible as possible to all users."

Italy (Garante)

- "In order for consent to be obtained lawfully, a controller will also be required to make sure that any mechanisms for giving one's consent online other than those proposed in these Guidelines are implemented in such a way as to make the effect produced by each action unambiguous for the user as well – to the extent such action is tantamount to the provision of consent. This is intended **to limit the occurrence of so-called 'false positives'**, i.e. random actions that are

misinterpreted as indications of the user's informed choice."

- "...one can easily dispel possible misunderstandings in interpreting the user's actions by having regard to the specific configuration of the buttons and colours used by publishers - which has hitherto not been unequivocal. In that regard, it is sufficient to reiterate that - **irrespective of the configuration adopted, the colours used for the buttons** and, ultimately, the implementing methods chosen - **the affirmative action the user is empowered to perform when first accessing a website must in any case be aimed at giving his or her consent (so-called 'opt-in')** and may never consist in refusing such consent (so-called 'opt-out')."

Luxembourg (CNPD)

- "Consent can only be valid if users are able to exercise their choice genuinely and freely, without being forced in any way to accept the use of cookies."

- "The CNPD recalls that data controllers must avoid misleading – consciously or not – users when seeking their consent."

- "It therefore recommends that the operators of websites or applications present, in an **identical manner,** the different choices available to the user regarding the acceptance of cookies."

- "In particular, the CNPD recommends avoiding the use of some or all of the following deceptive design practices, which are designed to trick the user and are part of the **"dark patterns"** phenomenon:
  - **Different contrasts of the 'consent buttons'** (e.g. the 'I accept' button has a high contrast making it clearly visible, whereas the 'I refuse' button has a very low contrast with the rest of the banner, and is therefore not very visible)".

Spain (AEPD)

- "The colour or contrast of text and buttons (or equivalent mechanisms) shall not be obviously misleading to users, in such a way as to lead to an involuntary consent. It **shall not be valid,** for example, if the option to reject cookies is a button with a text that **does not contrast sufficiently with the button's colour** and is therefore not readable."

National DPA Decisions

Austria (DSB)

- In case C037-10405, the DSB stated that a 'reject' option cannot be considered equivalent to the 'accept' option when it visually merges with the background colour of the consent banner and thus looks less prominent.

Bavaria (BayLDA)

- In case C037-11942, the BayLDA held that, notwithstanding the clear differences in colour and contrast (and also size and style), a reject option could still be perceived as a valid alternative to the accept option by the user, which makes the banner still acceptable.

Berlin (BInBDI)

- In case C037-12299, the BInBDI held that the accept and reject options must have the same 'Kommunikationseffekt', that is, it must be unequivocally clear from the way in which the button is designed that this will lead to a certain effect. In the BInBDI's view this is a mere matter of perception and it is irrelevant that the accept and reject options are not identical in colour, style or contrast, since what is more important is that the user is able to recognise the options as such.

France (CNIL)

- In case C037-10519, the CNIL considered the option to reject cookies designed as a grey on white link 'continue without accepting' in the right top corner of the banner to be lawful. According to the CNIL, even though the options differed in colour and contrast, their design could not be considered deceptive and it proved as easy to grant as to withdraw one's consent. Notably, this is in contrast with the DSB position referred to above.

Hessen (HBDI)

- In case C037-11052, the HBDI was satisfied with the controller's adaptation of their consent banner so that it displayed the reject option in the same form, colour, size and writing as the accept option, so that they could be considered as equivalent alternatives. The HBDI did not specifically mention the button's contrast.

Luxembourg (CNPD)

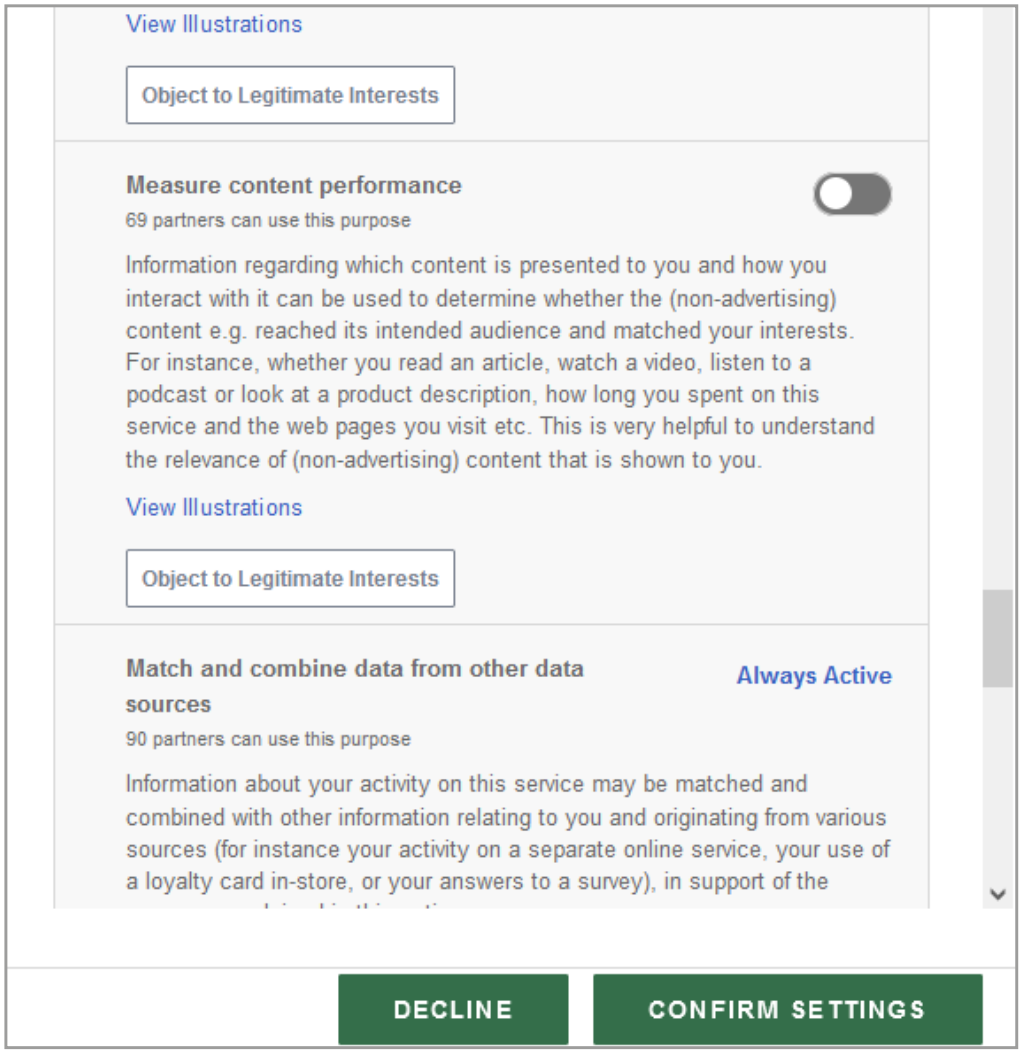
- The CNPD held, in case C037-10706, that it was satisfied with the website operator's adaptation of the consent banner solving this issue.

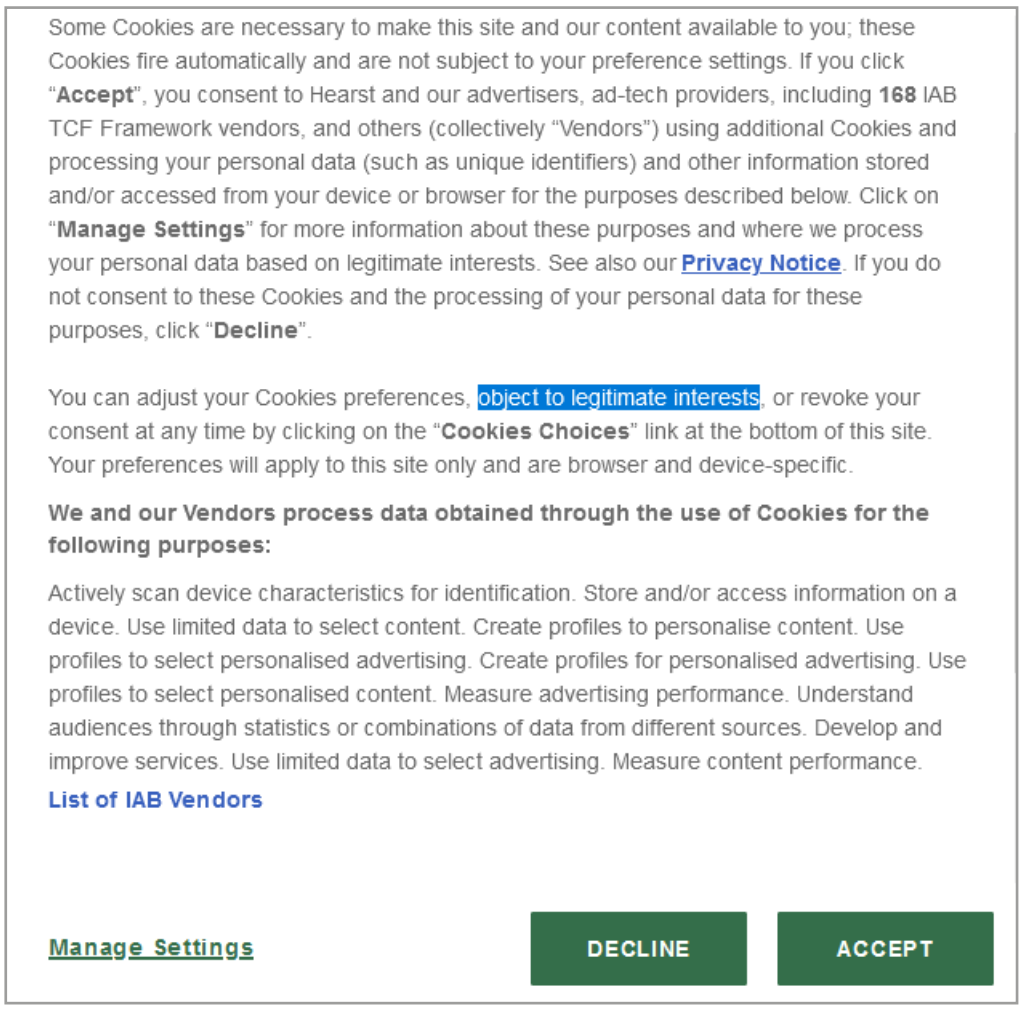
3.6. Issue 6: Legitimate Interest Claimed

Issue
Legitimate interests according to Article 6(1)(f) GDPR are invoked for processing activities mentioned in the consent banner.

However, under Article 5(3) ePrivacy Directive, the legal basis for the storing and the gaining access to information stored in terminal equipment is consent as per Article 6(1)(a) GDPR. Under this provision, a controller cannot rely on its legitimate interests for this processing.

Even if Article 6(1)(f) GDPR would be the adequate legal basis, no option to 'object' on the first layer, nor any other way to facilitate the right to object, is available in most cases. If no consent is given in the consent banner, it would be intuitive to assume that the person also objects to the processing according to Article 21 GDPR. However, in this case a double opt-out (refusing consent and objecting) would be necessary.





EDPB Report on the Work Undertaken by the Cookie Banner Taskforce

"In those cases, it appears that:

- The controller relied on legitimate interests under article 6(1)(f) GDPR for different processing activities as, for example, 'Create a personalised content profile' or 'Select personalised ads' whereas **it could be considered that no overriding legitimate interest would exist for such processing activities.**

- The integration of this notion of legitimate interest for the subsequent processing 'in the deeper layers of the banner' **could be considered as confusing for users who might think they have to refuse twice** in order not to have their personal data processed."

"The taskforce members agreed that whether the subsequent processing based on cookies is lawful requires to determine if:

- the storage/gaining of access to information through cookies or similar technologies is done in compliance with Article 5(3) ePrivacy directive (and the national implementing rules).

- any subsequent processing is done in compliance with the GDPR.

"24. In this regard, the taskforce members took the view that non-compliance found concerning Art. 5 (3) in the ePrivacy directive (in particular when no valid consent is obtained where required), means that the subsequent processing cannot be compliant with the GDPR. Also, the TF members confirmed that the legal basis for the placement/reading of cookies pursuant to Article 5 (3) cannot be the legitimate interests of the controller."

"25. The TF members agreed to resume discussions on this type of practice should they encounter concrete cases where further discussion would be necessary to ensure a consistent approach"

National DPA Guidelines

Belgium (GBA/APD)

- The processing of personal data in connection with the installation and reading of statistical cookies **cannot be based on the legitimate interest** of the owner of the website or application.

Czech Republic (UOOU)

- "Is it possible to process personal data through cookies based on **legitimate interest?**
- **Yes.** The **obligation to obtain consent for the use (storing and reading) of non-essential cookies** is imposed on website operators by the Czech Electronic Communications Act. This needs to be **distinguished from the subsequent processing of personal data** (analysis, profiling, etc.), which is fully subject to the regime of the General Data Protection Regulation. A website operator that uses cookies must therefore be able to rely on a legal basis for the subsequent processing of data, which in the case of cookies can be the consent of the data subject, legitimate interest, or processing necessary for the performance of a contract. An example of a legitimate interest is the processing of personal data for the purposes of first-party analytics (through the cookies of the website in question). However, if the user does not consent to the storage and reading of non-essential cookies, the operator is not authorized to use these cookies and, logically, subsequent processing of the user's personal data obtained through cookies cannot occur."

Denmark

- The Danish guidelines refer to the Article 29 Working Party Opinion No 6/2014 on legitimate interests (WP217).

Finland (Traficom – Transport and Communications Agency)

- "It should be noted **that legitimate interest does not authorise the storing or use of cookies or other data concerning the user's interaction with online services.** Rather, this must be based on the grounds listed in section 205 of the Act on Electronic Communications Services (917/2014). The section in question and the underlying Article 5(3) of the Directive on privacy and electronic communications do not recognise legitimate interest as a basis for storing or using cookies or other data on the user's interaction with online services on user devices. This means **that legitimate interest is not a valid ground** for using cookies or similar tracking technologies."

Germany (DSK)

- "In the context of tracking, the requirements of Article 6(1)(f) of the GDPR **are only met in a few circumstances in practice.**"

- "The balancing of interests within the scope of Art. 6(1)(f) of the GDPR **requires a substantial examination** of the interests, fundamental rights and freedoms of the parties involved and must be related to the specific individual case. Although **blanket statements that data processing is permissible under Article 6(1)(f) of the GDPR do not meet these legal requirements, they can often be found in data protection declarations of telemedia providers.**"

- "Furthermore, in cases where third-party service providers are involved in tracking as processors, it is important to consider whether these service providers also process data of the data subjects for their own purposes (e.g. to improve their own services or to create interest profiles). In this case - and even if the third-party service provider only reserves the right to do so in the abstract - the framework of a commissioned processing according to Article 28 GDPR is exceeded. **For the transmission of personal data** - even if it is only the IP address - to these third party service providers, **Art. 6(1)(f) of the GDPR can then generally not be an effective legal basis.**"

- "Since this legal basis can regularly only be used in individual cases and only in the context of a correspondingly meaningful balancing, the examination of the prerequisites will not be further deepened in this guidance. However, the explanations in the OH Telemedien 2019 can in principle still be used as a standard for review.

Italy (Garante)

- "One initial key conclusion can be drawn from the above analysis of the applicable legislation – namely, that the specific rules applicable to the specific processing situations do not envisage legal bases for such processing other than the data subject's consent or the fulfilment of any one of the conditions for derogating from the obligation to gather such consent as provided for in those rules. Accordingly, **under no circumstances will it be permitted to rely on the controller's legitimate interest to justify the use of cookies or other tracking tools** – contrary to what has been found in the course of the inquiries carried out into several web sites."

National DPA Decisisons

As a premise, it is worth stating that not many DPAs dealt with this issue in their decisions.

Berlin (BInBDI):

- The BInBDI concluded in case C037-10365, that a controller cannot rely on Article 6(1)(f) GDPR as a legal basis and at the same time ask for consent through the consent banner for a marketing cookie. In the DPA's view, this impacts the validity of consent and does not comply with Articles 13 and 14 GDPR. The BInBDI however, did not deal with the question whether the controller could lawfully claim a legitimate interest for third party services.

NRW (LDI):

- In its decisions, the LDI did not analyse further whether the controller violated the GDPR by relying on the legitimate interest legal basis since the controller adapted its website and stopped relying on this legal basis.

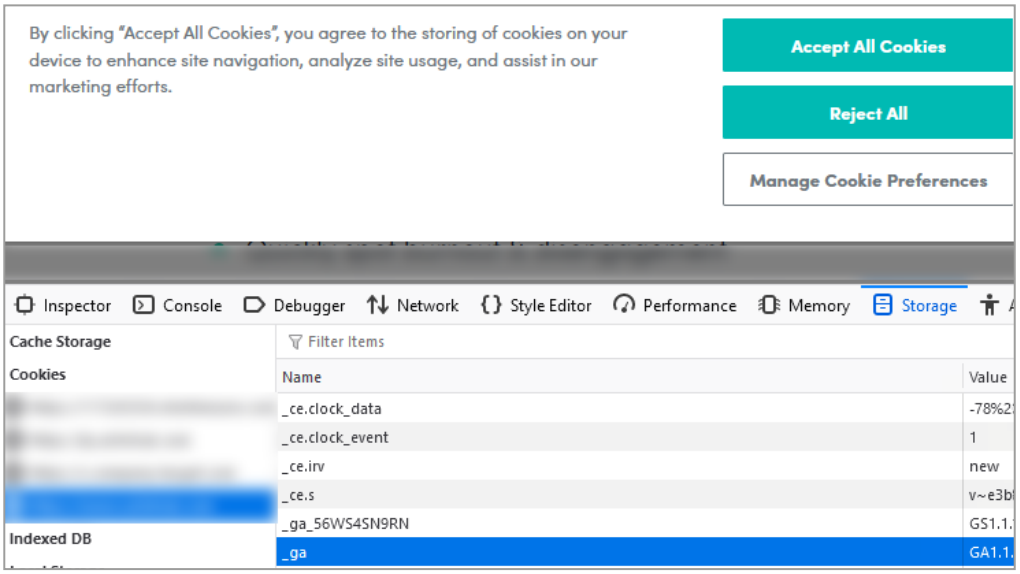
Spain (AEPD):

- The AEPD, in case C037-12417, held that cookies, where these do not amount to strictly necessary technical cookies, require consent for the processing to be lawful.

3.7. Issue 7: Inaccurately Classified Cookies

Issue
Certain cookies are classified as 'essential' or 'strictly necessary' when they are not. Therefore, there is no option to reject these processing operations and the controller is able to store and gain access to information in the equipment of users before any interaction with the consent banner.

This practice violates Article 5(3) ePrivacy Directive as well as Article 6(1) GDPR as it consists of storing and gaining access to information in terminal equipment of users that is not 'strictly necessary' without consent of the data subject.



Tracking-Cookie "_ga" is already installed before consenting.

EDPB Report on the Work Undertaken by the Cookie Banner Taskforce
"27. Taskforce members agreed that **the assessment of cookies to determine which ones are essential raises practical difficulties,** in particular due to the fact that the **features of cookies change regularly,** which prevents the establishment of a stable and reliable list of such essential cookies."

"28. The existence of tools to establish the list of cookies used by a website has been discussed, as well as the responsibility of website owners to maintain such lists, and to provide them to the competent authorities where requested and to demonstrate the 'essentiality' of the cookies listed.

"29. On that point, it has been mentioned that specific tools exist and may be used to analyse a website and create a report that shows all the cookies that were placed when visiting the website. However, the only available tools do not allow to check the nature of the cookies but only to list the cookies placed in order to ask the website owner to provide documentation on their purposes. These tools are thus an additional help for the competent authorities to seek further clarifications and

information from the website owners in addition to the information also provided on the website."

"30. The opinion n°04/2012 on Cookie Consent Exemption of WP 29 has also been recalled in relation to the criteria mentioned to assess which cookies are essential, and in particular the fact that cookies allowing website owners to retain the preferences expressed by users, regarding a service, should be deemed essential."

National DPA Guidelines

Austria (DSB)

- "It is not necessary to obtain the consent of the website visitor for the use of **'technically necessary cookies'.**"

- "Neither Directive 2002/58/EG nor the TKG 2021 contain a list of what is meant by 'technically necessary cookies'. However, the Opinion 04/2012 on Cookie Consent Exemption, WP 194, 00879/12/EN of the former Art. 29 Group sets some criteria for assessing whether cookies within the meaning of Art. 5 Para. 3 of Directive 2002/58/EC (...) are necessary from a technical point of view. The data protection authority recommends using the recommendations of the former Art. 29 WP in case of doubt."

- "From the data protection authority's perspective, the following services are necessary from a technical point of view (and corresponding cookies can therefore be set without consent):
  - Necessary session management (e.g. cookies to save the shopping cart as part of an online purchase or cookies to save the login status);
  - Entries in an online form if an entry on several subpages of a website is necessary to submit the form;
  - the information about the consent status, unless a unique online identifier is assigned for this."

- "From a technical point of view, **services that record and evaluate the online behaviour of people** on the respective website or across several websites or end devices are **not necessary** (and therefore require consent). From the point of view of the data protection authority, this includes in particular plugins from social media services or advertising networks, the implementation of which results in personal data of website visitors being transmitted to third parties."

- "According to the decisions of the DSB and the BVwG, Art. 5 Para. 3 of the Directive 2002/58/EG has **not** to be interpreted in the sense of an **'economic ne-**

cessity'. This means that advertising cookies do not become 'technically necessary' for the delivery of personalized advertising simply because the delivery of personalized advertising is necessary to fund the operation of the website (see the Judgment of the BVwG of March 12, 2019, GZ: W214 2223400-1)."

Belgium (GBA/APD)

- "If your websites or mobile apps that install and/or read cookies and other trackers from the computer, smartphone or tablet (or other terminal equipment) of your users, do you need to ask for their consent?
  - Yes, unless your website or application only use **'functional cookies'.**
  - A cookie is qualified as 'functional' when it is essential to send a communication via an electronic communications network or to provide a service expressly requested by the user of your website or application.
  - Here are some **examples** of 'functional cookies' for which you do not need to obtain the user's prior consent:
    - Cookies set for the duration of a session, or persistent cookies limited to a few hours in some cases, which are used to keep track of the information entered by the user when completing online forms on several pages or as a shopping cart to remember the items the user has selected by clicking a button.
    - Authentication cookies used for authenticated services (e.g. a site offering online banking services), for the duration of a session.
    - Security cookies which aim to reinforce the security of a service expressly requested by the user and which are used, in particular, to detect abusive authentications, for a repeated limited period.
    - Session cookies created by a media player, such as flash player cookies, for the duration of a session.
    - Load balancing session cookies, for the duration of a session.
    - Persistent user interface personalization cookies (such as cookies relating to language preference or results display preference), for the duration of a session (or slightly longer).
  - For the placement and/or reading of these functional cookies, you **do not need to obtain the user's consent.** But you must **nevertheless provide clear and precise information** about what these cookies do and why you use them."

Czech Republic (UOOU)

- "This is important so as to distinguish between situations where personal data are processed through **'essential cookies',** which are necessary for the website's own operation, and where the cookies are intended for monitoring traffic, analysis of the preferences of its visitors, e.g. for marketing purposes. etc., i.e. the so-called **'non-essential cookies',** which can be stored in end devices (and subsequently accessed) only on the basis of the consent of the user of this device, as stipulated in the Czech Electronic Communications Act."

Finland (Traficom – Transport and Communications Agency)

- "However, requesting consent is not required for setting up **essential cookies** or other similar technologies, i.e. when:
  - the **sole purpose** of storing and using the data is to **enable the transmission of messages** in communications networks or
  - the storage and use of the data is necessary for the service provider to provide a **service that the subscriber or user has specifically requested.** Even in this situation, storage and use of data is only allowed to the extent necessary to provide the service, and even then, protection of privacy may not be restricted any more than is necessary."

- "To be covered by the exception concerning the transmission of messages, the sole purpose of a cookie must therefore be to enable the transmission of messages. If cookies are only used to facilitate, speed up or in any way manage the aforementioned basic requirements, they are not covered by the exception. For the exception to apply, **the cookie must therefore directly enable or implement one or more of the following:**
  - implement the transmission of a message through a network, by (for example) identifying the transmission points required for routing the message
  - ensure the transmission of message content to the destination in an appropriate order
  - identify errors or data losses occurring during the transmission of the message."

- "Essential cookies may also be required **for the technical implementation of a user's specific request on a website.** The next section (Section 3.3) provides examples of different cookie types and guidance for the assessment on whether consent needs to be requested for their use."

Germany (DSK)

- "Section 25 (2) TTDSG provides **two exceptions** to the need for consent. The first one is primarily aimed at providers of telecommunications services within the meaning of Section 3 No. 1 TKG (new version). The second one, instead addresses the Telemedia providers pursuant to Section 2 para. 2 no. 1 TTDSG.
  - **Transmission of a message:** Pursuant to Section 25 (2) No. 1 TTDSG, consent is not required if the sole purpose of storing information or accessing information already stored in the user's terminal equipment is the transmission of a message via a public telecommunications network.
  - **Provision of a Telemedia service:** Section 25 (2) no. 2 TTDSG does not require consent if the storage of information or access to information already stored in the terminal equipment of a user is absolutely necessary so that Telemedia service providers can provide a service expressly requested by the user."

- "The term 'absolutely necessary' is neither defined in the TTDSG nor in the ePrivacy Directive in detail. However, the explanatory memorandum to the TTDSG assumes a **technical necessity,** which suggests a **strict understanding.** This means that even for services expressly requested by end users, access to the end device of the user is only covered by the exception when it is technically necessary to provide the desired service. This is so because the criterion of necessity within the meaning of the provision refers exclusively to the functionality of the Telemedia service as such. An exception to the consent requirement **cannot therefore be justified by the fact** that the that the storage of or access to information in the end device of a user **is economically necessary** for the business model of the Telemedia service."

Ireland (DPC)

- "Which cookies are exempt from the requirement to obtain consent from the user or subscriber? As a controller, you are potentially using cookies for analytics purposes or for marketing, targeting or profiling purposes and you may choose to assign them to certain categories when you provide information for users on your website. However, regardless of how you choose to categorise them, cookies that do not meet one of the **two specific use cases in the ePrivacy Regulations that make them exempt from the need to obtain consent** must not be set or deployed on a user's device before you obtain their consent."

- "The two exemptions are known as **a) the communications exemption** and **b) the strictly necessary exemption.**"
  The guidance explains further – providing examples – see page 8.

Luxembourg (CNPD)

- "In accordance with Article 4.3, e) of the amended law of 30 May 2005, there is no obligation to obtain the user's prior consent to the reading or placing of a cookie on his or her terminal equipment if the latter:
  — Is 'exclusively for the purpose of carrying out the **transmission of a communication** by means of an electronic communications network'.or
  — is **'strictly necessary** for the provider to supply an information society service expressly requested by the subscriber or user'."

- "In these guidelines, these cookies are referred to as 'essential cookies'."
  The guidance provides examples –see page 8 onwards.

Netherlands (AP)

- "As a website owner, you must inform visitors to your website about the placing and/or reading of cookies on their device. Then, in many cases, you have to ask the visitors' permission to do so. With tracking cookies, you must always do so."

- "**Functional cookies** are technically necessary for the website to work properly. Think of using a cookie to remember the contents of a shopping cart. As a website owner, **you do not need permission** to set these cookies. However, it is recommended that you inform your website visitors about these cookies."

- "**Analytical cookies** provide insight into the functioning of a website. As a website owner, **you do not need permission** to place analytical cookies that you only use to count visitors."

Spain (AEPD)

- "In such cases, if the cookies intended to be used are not **necessary for the operation of the service or application,** users must be allowed to give their consent before downloading the service or application. It should be recalled that in the case of websites offering audiovisual content, this is part of the **service expressly requested by the user,** and is therefore exempt the duty to obtain consent in order to display such content."

National DPA Decisions

Austria (DSB)

- The DSB held in its decisions that what should be seen as 'technically necessary cookies' needs to be interpreted strictly and from the point of view of the user, not of the service provider. Accordingly, the DSB held analytics cookies not to be 'necessary cookies'.

Luxembourg (CNPD)

- The CNPD held, in case C037-10706, that it was satisfied with the website operator's adaptation which avoids inaccurately classified cookies.

NRW (LDI)

- In its decisions, the LDI did not provide more information than stating that since the websites were adapted, it could not establish a violation in this regard.

Spain (AEPD)

- The AEPD, in case C037-12417 (available at: https://www.aepd.es/informes-y-resoluciones/resoluciones?search_api_fulltext=PS-00079-2023&sort_bef_combine=fecha_publicacion_DESC), held, making reference to the WP29 Opinion 4/2012, that analysis or performance and orientation cookies that had been installed obtaining consent, cannot be considered necessary and thus do require consent.

3.8. Issue 8: Not as Easy to Withdraw as to Give Consent

Issue
No option to withdraw consent can easily be found, for example with a 'withdraw' banner or a similar permanently visible option.

In accordance with Article 7(3) GDPR, it should be as easy to withdraw as to give consent. Therefore, if there is a prominent permanently visible consent option, there must be a similarly prominent withdrawal option.

Some websites found solutions to this issue, by adding a floating icon at the bottom of the page for example:

EDPB Report on the Work Undertaken by the Cookie Banner Taskforce
"31. It appears that where controllers provide an option allowing to withdraw consent, different forms of options are displayed. In particular, some controllers have not chosen to use the possibility to show a small hovering and permanently visible icon on all pages of the website that allows data subjects to return to their privacy settings, where they can withdraw their consent."

"32. Website owners should put in place easily accessible solutions allowing users to withdraw their consent at any time, **such as an icon (small hovering and permanently visible icon) or a link placed on a visible and standardized place.**"

"35. However, **website owners can only be imposed that easily accessible solutions are implemented and displayed once consent has been collected, but they cannot be imposed a specific withdrawal solution,** and in particular to set up a hovering solution for the withdrawal of consent to the deposit of cookies and other trackers. **A case-by-case analysis** of the solution displayed to withdraw consent will always be necessary. In this analysis, it must be examined whether, as a result, the legal requirement that it is as easy to withdraw as to give consent is fulfilled."

National DPA Guidelines

Austria (DSB)

- "Withdrawal option: The consent banner must clearly describe where and how the consent can be withdrawn. **Withdrawing must be as simple as giving consent.**"

Belgium (GBA/APD)

- "User-friendly solutions must be implemented so that individuals can withdraw their consent at any time **as easily as they gave it.** They must also be informed of this possibility when they give their consent."

Czech Republic (UOOU)

- "Consent to the processing of personal data can **be revoked by the data subject at any time,** and withdrawing consent must be as easy as giving it. Where consent is given via a consent banner, it is not acceptable if the withdrawal of consent is only possible, for example, by telephone. Ideally, **there should be an easily accessible button or link** on the website through which consent can be withdrawn."

Denmark (Datatilsynet)

- "Consent does not generally expire, but the controller must ensure that the data subject can **withdraw their consent at any time as easily as they have given it.**"

Finland (Traficom – Transport and Communications Agency)

- "According to the GDPR, users must be able **to withdraw their consent at any time.** Withdrawing consent or changing settings set earlier **must be as simple** for the user as possible. If consent is obtained electronically through a single mouse click, screen swipe or button press, users must be able to refuse or withdraw consent just as easily."

France (CNIL)

- "Users who have given their consent to the use of trackers **must be able to withdraw it at any time.** The Commission recalls that **it should be as easy to withdraw consent as to give it.**

- Users must be informed in a simple and intelligible way, even before they give their consent, of the options available to them to withdraw it.

- In practice, the Commission recommends that solutions allowing users to with-

draw their consent should be easily accessible at any time. The ease of access can be measured, inter alia, by the time spent and the number of actions required to effectively withdraw consent.

- The possibility of withdrawing consent may, for example, be offered **via a link accessible at any time** from the service concerned. It is recommended to use a descriptive and intuitive name such as 'cookie management module'. The publisher of a website may also provide users with a **'cookie' module accessible on all pages of the website by means of a 'cookie' icon,** for example at the bottom left of the screen. The publisher of a website may also provide users with a parameter-setting module accessible on all pages of the site by means of a **'cookie' icon,** located for example at the bottom left of the screen, allowing them to access the mechanism for managing and withdrawing their consent.

- In any case, the Commission recommends that the mechanism for managing and withdrawing consent be **placed in an area that attracts the attention of users** or in areas where they expect to find it, and that the visuals used are as explicit as possible.

- Finally, in order for the withdrawal of consent to be effective, it may be necessary to put in place specific solutions to ensure that previously used tracers are not read or written to."

Germany (DSK)

- "Since consent is revocable, a corresponding option for withdrawal must be implemented. Withdrawing consent must be as easy as giving it, Article 7(3) GDPR, fourth sentence."

- "If consent is given directly when using a website, **it must also be possible to revoke it in this way…** If consent was requested by means of a banner or similar, it is therefore also inadmissible that a data protection statement must first be opened and then scrolled in order to find a revocation option."

Greece (HDPA)

- "The user must be able to **withdraw his consent in the same way and with the same ease** with which he gave it."

Ireland (DPC)

- "The user must be able to withdraw consent **as easily as they gave it.**"

Italy (Garante)

- "Users will obviously be enabled to modify their choices, i.e., to give their con-

sent after they had withheld it and to withdraw their consent – at any time, **simply, easily, and in a user-friendly fashion** by way of an ad-hoc area that will be accessible through a link in the website footer; that link will have to flag the underlying purpose by way of wording such as 'Change your mind on cookies' or something of that kind."

- "It shall be understood that whenever the banner containing the short information notice and user options is displayed again as well as whenever the user changes his or her initial choices under the terms described above, any options selected on the occasion of subsequent accesses will have to override and supersede the previous ones – i.e., the new options will apply throughout regardless of whether consent is given after it had initially been withheld or consent is withdrawn after it had initially been given."

- "In order to ensure that users are not influenced or affected by design arrangements such as to lead them to prefer one option over the other, it is **fundamental additionally to rely on commands and characters of the same size, emphasis and colours** and that all such commands and characters are **equally easy to view and use.**"

Luxembourg (CNPD)

- "According to Article 7(3) of the GDPR, the data subject must be able to withdraw consent at any time and **as easily as he or she has given it.** This means that if consent can be given with one click, it must be possible to withdraw it as easily."

- "Later on, if the user wants to withdraw his consent, he should be able **to easily recall this same interface,** for example, through a clear link displayed at the bottom of each page, a floating icon or other quick and comprehensive means."

Spain (AEPD)

- "Users should be able to withdraw previously granted consent at any time. To this end, the publisher shall ensure that it **provides information to users in its cookie policy on how they can withdraw consent** and delete cookies."

- "The user should be able to revoke consent **easily.** The system provided for withdrawing consent should be **as easy as the system used when consent was given.** Such ease shall be deemed to exist, for example, where the user has easy and permanent access to the cookie management or configuration system."

National DPA Decisions

Austria (DSB):

- The DSB held, in case C037-10097, that there has to be a clear and simple indication on the initial banner, explaining how to withdraw one's consent. This should be clear to the user already at the moment of consent, as users cannot be expected to search through the whole website in order to find out how to withdraw their consent.

- As for the implementation of a withdrawal option, the DSB is of the view that a link at the end of each webpage or a clearly visible option in the menu suffice (see case C037-10187). Additionally, the DSB specified that in order for withdrawal to be as easy as granting consent, this should be possible without having to first uncheck a series of boxes.

Bavaria

- Bavarian DPA (BayLDA): With respect to the possibility to withdraw one's consent, the BayLDA held that the existence of a reference to this possibility in the consent banner and a link redirecting to the consent management options at the bottom of each page suffices to be considered a valid way to withdraw one's consent (see case C037-11942).

- Bavarian Regulatory Authority for New Media (BLM): In cases of its competence the BLM held, with respect to the withdrawal of consent, that the presence of a link named 'cookie settings' at the end of each webpage is to be considered in compliance with GDPR provisions as it is also in line with the position of the EDPB Taskforce.

Berlin (BInBDI):

- The BInBDI agrees in principle that it must be as easy to withdraw as to grant consent. Accordingly, the BInBDI held, in its decision on case C037-11207, that the fact that withdrawal of consent required more steps and search processes than granting consent and that there was no reference to the possibility of withdrawal in the text of the banner. This corresponds to the DSK point of view.

France (CNIL):

- In case C037-10519, the CNIL found that a link at the end of each page of the website in question could be considered a lawful permanent option to withdraw one's consent. Similarly, in case C037-11101, the CNIL accepted a link at the end of each page as a lawful option to withdraw one's consent but required the webpage operator to change the name of the link form 'manage my preferences' to 'manage my cookies' in order for it to be sufficiently clear that it allowed

users to change their cookie settings.

Hessen (HBDI):

- The HBDI held, in cases C037-14024 and C037-10408, that the implementation by the controller of a hovering icon, as suggested by noyb, that redirects users to the privacy settings of the webpage allows for a lawful withdrawal of consent under Article 7(3) GDPR. Hence, in these cases, the controllers decided to follow noyb's suggestion without the need for the DPA to adopt any measures against them.

Luxembourg (CNPD)

- The CNPD held, in case C037-10706, with respect to noyb's submission that the issue persisted even after the adaptation of the website by the controller, that a footer link or a hovering icon on each page, redirecting users to the consent management settings is sufficient to satisfy the requirements of Article 7(3) GDPR. This, according to the CNPD, is justified by the fact that the consent banner clearly informs users on how to withdraw their consent and the link in question is sufficiently visible for them, thus it did not consider it necessary to impose on the website operator to adopt a hovering icon option.

NRW (LDI):

- In its decisions, the LDI generally represents the position taken by the German DPAs in the DSK, that the withdrawal of consent shall be as easy as granting it. However, the LDI, although agreeing that a hovering icon would be the optimal solution, stated it cannot impose this on controllers. For the LDI it suffices that a link at the end of the webpage exists, redirecting the user to the banner where the reject option is available.

Spain (AEPD):

- In the AEPD's view, a lawful way to withdraw once consent is given, for example, when the user has easy access to the cookie management settings on a permanent basis through a link. In decision C037-10146, the AEPD fined a company EUR 5.000 because initially there was no option to access the consent management tool to withdraw one's consent and once this had been added the operator kept using non-necessary cookies even after withdrawal of consent.

4. Relevant EDPB Guidelines - Overview

4.1. Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them – Relevant extracts

Overloading – Privacy Maze
"Using the method of layered approach can help present the privacy notice more clearly in the sense of Article 12(1) GDPR. However, this should not result in making the exercise of important functions or rights **unnecessarily difficult** by providing a complex privacy policy consisting of **innumerable layers** that would result in the deceptive design pattern **Privacy Maze** […]".

"The layered arrangement is intended to facilitate readability and give information on how to exercise data subject rights, not to make them more difficult. It must therefore always be determined on a case-by-case basis whether too many layers are used and thus deceptive design patterns occur". […] "However, the higher the number, the more it can be assumed that users will be discouraged or misled".

"[…] However, this is to be assessed differently when it comes to the exercise of the rights of the users… users should get to the function that allows them to exercise their rights as directly as possible".

(3.2 Staying informed on social media - Use case 2a: A layered privacy notice - c. Deceptive design patterns - ii. Interface based patterns > Margin n. 79, 80, 81)

Obstructing – Dead End
"Violations of legal requirements can also occur when data protection information required by the GDPR is made available through further actions, such as clicking on a link or a button. In particular, **misdirected navigation or inconsistent interface** design **that leads to ineffective features** cannot be classified as fair under Article 5(1)(a) GDPR, as users are misled when they either try to reach some information or set their data protection preferences. Dead ends where users are left alone without functions to pursue their rights should therefore be avoided in any case and directly violate Article 12(2) GDPR stating that the controller has to facilitate the exercise of rights".

(3.2 Staying informed on social media - Use case 2a: A layered privacy notice - c. Deceptive design patterns - ii. Interface based patterns > Margin n. 84)

Obstructing – Longer than necessary
"Article 7(3) GDPR states that the withdrawal of consent should be as easy as giving consent. The Guidelines 05/2020 on consent under Regulation 2016/679 elaborate further on the matter by stating that **giving and withdrawing consent should be available through the same mean.** This entails using **the same interface,** but also implies that the mechanisms to withdraw consent should be easily accessible, **for example through a link** or an icon available at any time while using the social media platform.

- Example 33: A social media provider does not provide a direct opt-out from a targeted advertisement processing even though the consent (opt-in) only requires one click.

The time needed or the number of clicks necessary to withdraw one's consent can be used to assess if it is effectively easy to achieve. Implementing the deceptive design pattern **Longer than Necessary** within the user journey to withdraw their consent, as shown in example 33, goes against these principles, thus breaching Article 7 (3) GDPR."

(3.3 Staying protected on social media - Use case 3a: Managing one's consent while using a social media platform - b. Deceptive design patterns > Margin n. 115, 116)

Overloading – Privacy Maze
"[…] Social media providers need to **stay mindful of avoiding the Privacy Maze** deceptive design pattern when providing information related to a consent request in a layered fashion".

- Example 34: Information to withdraw consent is available from a link only accessible by checking every section of their account and information associated to advertisements displayed on the social media feed.

"As the scenario described above shows, the deceptive design pattern **Privacy Maze can also be an issue once consent is collected** … the **withdrawal of consent shall be as easy as to give consent.** This is specifically due to the fact that the process of withdrawal of consent includes more steps than the affirmative action of providing consent. As the given information is also not easily accessible to the data subject, as it is spread over different parts of the page, the principle as laid down in Article 12 (1) GDPR is violated."

(3.3 Staying protected on social media - Use case 3a: Managing one's consent while using a social media platform - b. Deceptive design patterns > Margin n. 117, 118)

Stirring
"Affecting the choice users would make by **appealing to their emotions** or using **visual nudges.**"

Emotional Steering
"Using wording or visual elements (such as **style, colours, pictures or others**) in a way that confers the information to users in either a **highly positive outlook,** making users feel good, safe or rewarded, or in a **highly negative one,** making users feel scared, guilty or punished. Influencing the emotional state of users in such a way is likely to lead them to make an actionthat works against their data protection interests".

Hidden in plain sight
"Use a **visual style** or technique for information or data protection controls that **nudges users toward less restrictive and thus more invasive options.**"

(Annex I: List of deceptive design pattern categories and types)

4.2. Other Relevant guidelines

EDPB Guidelines 8/2020 on the targeting of social media users

EDPB Guidelines 05/2020 on consent under Regulation 2016/679

EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Article 29 Working Party Guidelines on Transparency under Regulation 2016/679

Article 29 Working Party, Opinion on profiling and automated decision making

Article 29 WP, Opinion on legitimate interests

5. Methodology

The current report is limited to the experience that *noyb* had in relation to consent banners and European Data Protection Authorities. It also relates to guidelines and similar documentation issued by these Authorities. The information in the report is updated as of November 2023.

The case numbers mentioned throughout the report are the case numbers of *noyb*. The case numbers of Data Protection Authorities are not used as many of the relevant decisions are not published. They are therefore not helpful in finding the case in a public database. This is, for example, a common issue with German Data Protection Authorities but concerns many other Data Protection Authorities, too. With the *noyb* case number and the Data Protection Authority you can find more information about individual cases here: https://noyb.eu/en/project/dpa

Machine-based translation tools were used for translations from several languages to English.

All information provided was drawn-up to the best of our knowledge. However, this report solely gives an overview regarding different decisions. It does not provide detailed information of each decision. It should be taken into account that the legal assessment of Data Protection Authorities in comparable cases may also evolve over time. Furthermore, this report is not meant as legal advice.

European Center for Digital Rights

Imprint:
noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna – Austria
ZVR: 1354838270