guiding handbook

Cookies and personal data protection

Oct / 2022

ANPD Autoridade Nacional de Proteção de Dados

guiding handbook

Cookies and personal data protection

Alexandra Krastins Lopes
Andressa Girotto Vargas
Davi Téofilo Nunes de Oliveira
Isabela Maiolino
Jeferson Dias Barbosa
Lucas Borges de Carvalho
Marcelo Santiago Guedes
Thiago Moraes

Brasília, DF
2022

Version 1.0
Digital Publication (October / 2022)

ANPD
National Data Protection Authority
SCN, Qd. 6, Conj. A,
Ed. Venâncio 3000, Bl. A, 9th floor
Brasília, DF - Brazil - 70716-900
www.anpd.gov.br

Summary

Presentation

Every day, when entering an Internet page, we are avi- 5
that the *site* in question uses cookies. You may therefore need to accept, decline or manage preferences - in the latter case by indicating more specifically which categories of *cookies* and their purposes may be used by the service provider. *Cookies* now play an important role on the Internet, in some cases enhancing the user experience and supporting certain business models. Among other purposes, *cookies* enable web pages to function and services to be provided on the Internet, including measuring the performance of a web page and serving personalized advertisements.

Although the presentation of information related to the use of *cookies* is distinct and may vary greatly depending on the page accessed, by agreeing to the stipulated conditions, the user will be subject to some kind of tracking of activities performed on the internet, either by the person responsible for the site or by third parties. Therefore, as may occur with the use of similar technologies, the use of *cookies* without the proper technical and legal safeguards can have negative impacts on the rights and privacy of holders of personal data.

One of the potential problems related to the use of *cookies* is the lack of transparency, i.e., not providing clear, accurate and easily accessible information about the collection and processing, which may make it impossible or unduly restrict the holder's control over his or her personal data. Privacy risks may be magnified in situations where the lack of transparency is coupled with practices of collecting massive amounts of personal information for purposes of identifying, tracking, and profiling user behavior.

Considering these aspects, which denote both the importance and the risks involved in using *cookies* in the di- 6
gital, this Guide presents an overview of the subject, analyzes the main concepts and categories of *cookies,* and examines the legal hypotheses applicable and the requirements to be observed in the event of their use.

Furthermore, this Guide seeks to identify positive and negative practices in the development of *cookie* policies, more precisely regarding *cookie banners* inserted in websites, and also instructs such development by means of illustrative examples.

Although the Guide focuses primarily on the collection of personal data through *cookies* when accessing electronic pages on the Internet, the guidelines presented here are also generally applicable to the collection of personal data through the use of similar tracking technologies, including mobile devices (cell phones and tablets, for example), subject to the peculiarities of each context.

It is emphasized that compliance with the contents of this Guide does not exempt the processing agents from complying with the other precepts of Law No. 13,709, of August 14, 2018 - General Law for the Protection of Personal Data (lgpd) for the purposes of compliance, regularity and validity of the

operations and personal data processing activity, and to take the necessary steps to safeguard the rights of data subjects.

This Guide will be open to comments and contributions on a continuous basis, in order to update it in due course as new regulations and understandings are established, at the discretion of the ANPD. The suggestions can be sent to the ANPD Ombudsman, through the Platform Fala.BR (https://falabr.cgu.gov.br/).

Concept and classifications

What are cookies?

Cookies are files installed in a user's device that allow the collection of certain information, including personal data in some situations, in order to meet various purposes[1]. Among this information, many are essential for the proper and safe functioning of electronic pages and to enable the provision of services in the digital environment. For example, the use of *cookies* can identify a user before conducting an *online* transaction, or "remember" previous choices, such as the language used, the type of product preferred, passwords and logins used on websites, and products that were added to the cart to make a purchase. In addition, they can be used for other purposes such as measuring a page's audience and offering personalized advertisements.

It should also be noted that *cookies* allow a series of data to be stored on users' devices. The information collected and stored by *cookies* may refer directly to natural persons or indirectly allow their identification, for example, by making inferences and cross-referencing with other information, and sometimes through the formation of behavioral profiles.

mental data. In the latter case, it is possible to consider the behavioral profile as personal data, since it is associated with a natural person[2]. In this sense, in the cases mentioned above, personal information collected through *cookies* may be considered personal data, whose treatment is regulated by the lgpd.

Cookie categories

The categories for defining *cookies* are diverse and can come from different perspectives. In this Guide, some of them will be presented.
but of the most commonly used categories, in a non-exhaustive manner.
These are organized by the most common types of *cookies*. It is important to consider that the same *cookie* can be included in more than one category.

Thus, the following are the categories of cookies according to: (i) the entity responsible for their management; (ii) the need; (iii) the purpose; and (iv) the information retention period.

cookies in agreement with the entity responsible for their management

a. Own or first-party cookies: these are *cookies* set directly by the website or application that the data subject is visiting. First-party cookies generally cannot be used to track activity on a site other than the original site where it was placed. These types of *cookies* can include information such as *login* credentials, shopping cart items, or preferred language.

b. Third-party cookies: these are *cookies* created by a domain different from the one the owner is visiting. They arise from functionalities of other domains that are incorporated into an electronic page, such as the display of advertisements.

cookies as needed

c. Necessary *cookies*: these are ***cookies*** used for the website or application to perform basic functions and operate correctly. Therefore, the collection of the information is essential to ensure the functioning of the website or the adequate provision of the service. Thus, the activities covered as strictly necessary include those related to the specific functionality of the service, i.e. without them the user would not be able to perform the main activities of the site or application. This category is restricted to what is essential to provide the service requested by the titleholder, and does not contemplate purposes other than the provision of the service.
essential, which serve other interests of the controller.

d. *Cookies that* are not **necessary**: *cookies* that do not fall within the definition of necessary *cookies* and whose disabling does not prevent the website or application from working or the user from using the services. In this sense, non-essential cookies relate to non-essential functionality of the service, application or website. Examples of non-essential cookies include, but are not limited to, cookies used to track behavior, measure the performance of the page or service, and display ads or other embedded content.

It is worth noting that the distinction between required and non-required *cookies* is especially relevant to defining the legal assumption authorizing the use of *cookies* and the collection of personal data, such as consent and legitimate interest, as discussed in the next section of this Guide.

cookies according to purpose

e. Analytical or performance cookies: they make it possible to collect data and information about how users use the site, which pages

visit that site more frequently, the occurrence of errors or information about the performance of the site or application itself.

f. Functionality cookies: These are used to provide the basic services requested by the user and make it possible to remember website or application preferences, such as username, region or language. Functionality *cookies* may include own, third-party, persistent, or session *cookies.*

g. Advertising cookies: these are used to collect information from the owner for the purpose of displaying advertisements. More specifically
from the collection of information regarding the browsing habits of advertising *cookies* allow the user to be identified, profiles to be built, and ads to be displayed that are customized to the user's interests.

cookies according to the information retention period

h. Session or temporary *cookies*: These are designed to collect and store information while holders access a *website*. They tend to be discarded after the end of the session, i.e. after the user closes the browser. They are used on a regular basis to store information that is only relevant for the provision of a service requested by users or for a specific temporary purpose, as is often the case with a list of products in the shopping cart of a *website.*

i. Persistent cookies: The data collected via these *cookies* is stored and can be accessed and processed for a period defined by the controller, which can vary from a few minutes to several years. In this regard, it must be assessed on a case-by-case basis whether the use of persistent cookies is necessary, since the threats to the security of personal data can be very great.

Privacy concerns can be reduced through the use of session cookies. In any case, when persistent *cookies* are used, it is recommended to limit their duration in time as much as possible, taking into account the purpose for which they were collected and will be processed, as explained later in this Guide.

Cookies and the LGPD

General Aspects

Cookies are a useful mechanism for various purposes, including identifying users, enabling *online* payments, presenting ads and measuring the effectiveness of a service or a website. However, the fulfillment of these purposes will only be legitimate if the principles, the rights of the titleholders and the data protection regime foreseen in the lgpd are respected.

Personal data collected from interactions on a website, in an application, or in a digital service can reveal many aspects of an individual's personality and behavior. In such contexts, these individuals are placed in a more vulnerable position, especially in view of the asymmetry of information with respect to large Internet application providers that are responsible for processing a massive amount of personal data, or when the purposes of the processing are not presented in a clear, precise and easily accessible way.

Even before the publication of the lgpd, the Marco Civil da Internet (mci, Law No. 12,965/2014) had already recognized that, next to freedom of expression, the guarantee of privacy and protection of personal data should be guaranteed.

is an essential condition for the full exercise of the right of access to the network (arts. 3, 7 and 8). The MCI also established strong protection for personal data, by providing that their storage and availability *"must meet the preservation of the intimacy, private life, honor, and image of the parties directly or indirectly involved*. Furthermore, the availability of connection and access records to internet applications, even when associated to personal data, to public authorities or third parties, may only occur, as a rule, by means of court order[13].

The protective provisions of the MCI were extended by the LGPD, standard which provided for the protection of personal data in a more comprehensive manner [14]

This includes rights for data subjects, guiding principles for processing personal data, and obligations for data processors. Among the main provisions of the GDPR applicable to the collection of personal data through *cookies* or other *online* tracking technologies are the following:

(i) **Principles of purpose, necessity and adequacy** (article 6, i, ii and iii): the collection of personal data through the use of *cookies* must be limited to the minimum necessary for legitimate, explicit and specific purposes, observing the impossibility of further processing in a manner incompatible with these purposes. In this regard, the purpose that justifies the use of a given category of *cookies* must be specific and informed to the owner, and the collection of data must be compatible with this purpose. For example, if the party responsible for the website informs the owner that it uses *cookies* only for audience measurement purposes, it cannot use the information collected for other purposes that are not compatible with this purpose, such as profiling and advertising. Likewise, it may not collect other personal data that is not related to or compatible with this purpose. Therefore, it is not admissible to

indication of generic purposes, such as the request to accept general terms and conditions, without indicating the specific purposes for which the *cookies* will be used. Furthermore, the principle of necessity dictates that processing should cover only *"data* that are *relevant, proportionate and not excessive in relation to the purposes of the data processing*. This principle advises against the actual processing of personal data where the purpose can be achieved by other means that are less burdensome for the data subject.

(ii) **Principles of free access and transparency** (art. 6, iv and vi): implace an obligation on the processing agent to provide the entitled persons with the necessary information.
lares clear, precise and easily accessible information on the form of treatment, the retention period and the specific purposes that justify the collection of their data by means of *cookies*. It is also important that information is provided on the possible sharing of data with third parties and on the rights assured to the holder, among other aspects indicated in art. 9 of the lgpd.

> *A good practice is to tell the owner how to manage cookie preferences in their own browser or device. Thus, for example, it can be explained how cookies can be deleted or how to disable third-party cookies. It is important to note that the management of cookies by the browser has a complementary function, which does not remove the need to provide the holder with a direct and proper mechanism for managing cookies and exercising their rights, always accompanied by the corresponding information. As to the form of presentation, this information may be indicated, for example, in banners, presented after access to a web page; and, in a more detailed manner, in privacy policies or notices, containing information about the policy*

> *cookies used by the processing agent, according to the recommendations presented in this Guide.*

(iii) Holder rights: among others, particularly relevant in the context of the use of *cookies* are the rights of access, deletion of data, revocation of consent and opposition to processing, always by means of a free and facilitated procedure, as provided for in art. 18 of the lgpd.

> *To meet this legal determination, it is recommended to provide the holder with a mechanism for "managing cookies", whereby it is possible, for example, to review per- sonal data. This may include the revocation of consent related to the use of cookies for marketing purposes, when that is the legal basis used.*

It is important to emphasize that, regardless of the technology used, practices that imply the indiscriminate collection of personal data - without a purpose that is specifically defined and clear to the data subject - and the corresponding unlimited tracking of data subjects in the digital environment are not compatible with the lgpd. The violation of the rights of the data subject will occur, especially when the collection is not supported by an appropriate legal hypothesis and clear, precise and easily accessible information is not made available to give the data subject the effective possibility of understanding and controlling the use of his or her personal data.

(iv) Termination of processing and erasure of personal data: the lgpd provides that, as a general rule, personal data must be erased after the end of processing, which may occur, for example, when the purpose is achieved or erasure is legitimately requested by the data subject. Thus, the storage of personal information after the end of the processing only applies when the purpose of the processing has been achieved.

is admitted in exceptional cases, such as for purposes of compliance with a legal obligation, among other hypotheses foreseen in art. 16 of the lgpd. It follows that the *cookies* retention period must be compatible with the purposes of the treatment, being limited to what is strictly necessary to achieve this purpose. Therefore, retention periods that are indeterminate, excessive or disproportionate in relation to the purposes of the processing are not compatible with the GDPR.

(v) Legal hypotheses: these are the hypotheses in which the lgpd authorizes the processing of personal data, as provided in art. 7 and in
Art. 11, this in the case of sensitive personal data. So, always 17 which involves the processing of personal data, the use of *cookies* may only be admitted if the legal hypothesis applicable by the controller is identified and the specific requirements stipulated for this purpose in the lgpd are met.

Legal hypotheses[4]

Two legal hypotheses will be presented below, consent and legitimate interest, the most usual and relevant to the context analyzed. The indication made in this Guide is not exhaustive, since the collection of personal data through cookies may eventually be supported by other legal assumptions, provided that the requirements set forth in the lgpd are met.

consent

According to the lgpd, consent must be free, informed and unambiguous. Consent is free when the data subject actually has a choice about the processing of his or her personal data.

That is, you must be assured of the effective possibility of accepting or refusing the use of *cookies,* without negative consequences or controller inter- ventions that could vitiate or impair your expression of will.

Due to this legal requirement, it is not compatible with the GLPD to obtain "forced" consent, i.e., conditioned to the full acceptance of the conditions of use of *cookies*, without providing effective options to the holder. It should be noted, however, that the regul- larity of consent should be verified according to the text and peculiarities of each concrete case, considering, in
particular, whether the holder is provided with a real and satisfactory alternative. [18]

Consent must also be informed, requiring that the data subject be provided with all the information necessary to make an informed assessment and decision regarding whether or not to consent to the use of *cookies*. Thus, as already mentioned, the data subject must be provided with clear, precise and easily accessible information about the form of the treatment, the retention period and the specific purposes that justify the collection of their data by means of *cookies*, among other information indicated in article 9 of the lgpd.

It is important to emphasize that this information is linked to the very use of the personal data. Any change in the assumptions adopted for obtaining consent taints the legal assumption adopted, requiring new consent by the data subject, or the use of another legal assumption, in accordance with the new assumptions established and with all the necessary information for this purpose.

In addition, consent must be unambiguous, which requires obtaining a clear and positive manifestation of will from the data subject, not admitting its inference or obtaining it in an unequivocal way.

tacit or from an omission by the holder. Therefore, given the incompatibility with the provisions of the lgpd, we do not recommend the use of *cookie banners* with pre-selected authorization options or the adoption of tacit consent mechanisms, such as the assumption that by continuing to browse a page, the data subject would provide consent to the processing of their personal data.

In the case of collection of sensitive data on the basis of the holder's consent, it is necessary that, in addition, consent be obtained in a specific and prominent manner, as provided for in art. 11, i,
of lgpd. Regarding the highlighted form, it is recommended that the authori- 19
In the case of sensitive data, the notification for processing sensitive data must either be separate from the main text or a means must be used to highlight it so that it indicates what sensitive data will be collected and for what specific purpose it will be used by the data controller.

In any case, a simplified and free of charge procedure to revoke the consent provided for the use of *cookies* must be made available to the holder, similarly to the procedure used to obtain it. In this sense, art. 8, §5, of the lgpd establishes that *"consent may be revoked at any time upon express manifestation of the holder, through a free and facilitated procedure"*. The revocation act is unilateral and must be attended to whenever requested by the holder.

It is important to note that it is the responsibility of the controller to prove that consent was obtained with respect to all the parameters established by the lgpd. Thus, it is good practice to record and document all the requirements necessary to prove that the consent is unbiased and contains all the necessary information.

In view of what these legal requirements establish, it is not appropriate to use the legal hypothesis of consent in the case of strictly necessary *cookies.* This is because, in these cases, the collection of the information is essential to ensure the operation of the website or the adequate provision of the service, so that there are no effective conditions for a free manifestation of the holder or even to ensure him/her the real possibility to choose between accepting or refusing the processing of his/her personal data.

Similarly, consent will not be the appropriate legal hypothesis.
if the processing is strictly necessary for the fulfilment of 20
legal obligations and attributions, especially when the existence of a clear and direct link between data collection through *cookies* and the exercise of typical state prerogatives by public entities and agencies is demonstrated[5]. In any event, the owners must be provided with the relevant information, in accordance with the principles of transparency and free access, besides being assured the exercise of their rights and observing the provisions of art. 23 of the lgpd.

Thus, while there is no hierarchy or preference among the legal scenarios set forth in the GDpL, the use of consent will be more appropriate when information is collected via non-required *cookies*. In these situations, the collection of the information is not essential to the adequate provision of the service or to ensure the operation of the website. In fact, as seen above, non-essential cookies are related to non-essential functionalities of the service or web site, such as the display of ads or behavioral profiling. In such cases, it becomes possible to provide the user with a genuine choice between accepting or refusing the installation of *cookies* for one or more of these purposes, a central prerequisite for the use of the legal assumption of consent.

example 1

Collecting cookies from a supermarket website

When accessing a supermarket's website to purchase a product, the user is directed to a banner that states that "this site uses cookies to improve your experience, gather usage statistics, and deliver relevant ads to you". No additional information is presented and the only option provided is expressed in the "I agree" box.

Analysis - The *cookies* whose collection is informed by the banner available to you
level on the supermarket's website are characterized as cookies not required, where the data controller has chosen to request the data subject's consent. However, providing a single option to the data subject, without the possibility to refuse the use of *cookies that* are not necessary, goes against the requirement that consent should be freely given. Furthermore, the absence of clear, precise and easily accessible information on, inter alia, the specific purposes of the processing and the data retention period, violates the legal requirement that consent must be informed. Finally, the failure to provide a simplified and free mechanism for the revocation of consent at any time by the data subject is also a practice incompatible with lgpd.

example 2

Adaptation of a school's website to the LGPD

A school received a complaint from a parent association about a lack of transparency in the collection of personal data through cookies on its website. The user accessing the page was presented only with a banner with the button "I understand" accompanied by the information "by clicking 'I understand', you agree to the storage of cookies".

We use cookies on your device to improve navigation on the site and our services, as well as to assist our marketing efforts. After conducting studies and identifying best practices, with the cooperation of the administrator and the support of senior management, the new version of the school's website presents the user with a banner that reads: "this site uses cookies necessary for its operation. If you provide your consent, we will also use cookies to collect data that will enable the display of personalized advertisements." In addition to this information, the banner now has three options, all in the same format and highlighted: "accept-all cookies"; "reject all cookies"; and "manage cookies".

By clicking on this last option, the user is directed to a banner which contains more detailed information about the use of cookies, such as their specific purposes and retention period. Consent-based cookies are disabled by default, with the possibility for the user to select the options they deem appropriate for the collection of their personal data.

Analysis - The possibility of accepting or refusing the use of *cookies* that are not necessary, independently of necessary *cookies,* allows consent to be free. In addition, the new *banners* now provide clear, precise and easily accessible information on, among other things, the specific purposes of processing and the data retention period, in compliance with the legal requirement that consent must be informed. Additionally, in accordance with the provisions of the lgpd, consent-based *cookies* are disabled by default. Finally, the only thing missing for the page to be lgpd compliant was a simplified and free mechanism for the holder to revoke consent at any time.

legitimate interest

The legal hypothesis of legitimate interest authorizes the processing of personal data of a non-sensitive nature when necessary to meet the legitimate interests of the controller or of third parties, *"except when fundamental rights and freedoms of the data subject prevail and require protection of personal data"* (art. 7, ix).

The controller's interest will be considered legitimate when it is compatible with the legal system and does not contradict the provisions of the law. In addition, the controller must assess, at the time
prior to performing any operation based on legitimate in- 23
if, in the case in question, the fundamental rights and freedoms of the data subject are overriding and require protection of personal data and therefore require the processing to be carried out. As in any data processing operation, it is also important to prove the adoption of technical and administrative measures capable of safeguarding the operation and the data used, ensuring the security of the processing and transparency for the data subjects.

The assessment to be made by the controller of the data subject's legitimate expectations must take into account the respect for the data subject's individual rights and freedoms. In order for the processing to be adequate, the controller must make sure that the intended use, in addition to not infringing rights and freedoms, could be reasonably foreseen by the data subject, that is, that it would be possible for the data subject to assume that such use could occur with his or her personal data based on the information provided by the controller at the time of the collection of the personal data. Furthermore, it should be considered that, according to art. 18, § 2, the data subject has the right to oppose processing carried out on the basis of legitimate interest, in the event of non-compliance with the requirements foreseen in the lgpd.

In general, legitimate interest may be the appropriate legal hypothesis in cases of use of *cookies that* are strictly necessary, i.e., those that are essential for the proper provision of the service or for the operation of the website, which can be understood as a form of support and promotion of the activities of the controller and the provision of services that benefit the holder (art. 10, i and ii, lgpd). The analysis, however, must consider the peculiarities of each concrete situation and assess whether, in this case, the rights and interests of the titleholders do not prevail, observing the other applicable legal requirements.

In the case of the public sector, the legal assumption of legitimate public interest is

The collection of personal data by means of *cookies may be* supported, except, according to orientation already signed by the anpd, in case of a clear and direct link between the processing and the exercise of typical state prerogatives, resulting from the fulfillment of legal obligations and attributions[6].In any case, the data subjects must be provided with the pertinent information, in conformity with the principles of transparency and free access, besides being assured the exercise of their rights and observing the provisions of art. 23 of the lgpd.

The use of *cookies* for audience measurement purposes (ana- lytic or measurement cookies) may be supported by the legal hypothesis of legitimate interest in certain contexts, subject in any case to the requirements set out in the lgpd. In particular, it is reasonable to assume that audience measurement will constitute a legitimate interest of the controller, as well as that the risks to the privacy of data subjects will be lower when the processing is limited to the specific purpose of identifying patterns and trends, based on aggregate data and not combined with other tracking mechanisms or user profiling.

On the other hand, it is possible to state that legitimate interest will hardly be the most appropriate legal hypothesis in cases in which the data collected through cookies are used for advertising purposes. This is especially the case when the collection is made through third party *cookies* and when associated with practices that may involve greater risk to the privacy and fundamental rights of the owners, such as behavioral profiling, analysis and prediction of preferences and behavior, or even tracking of the user by different electronic pages.

In such contexts, the balancing test under lgpd will generally lead to the conclusion that rights and freedoms should prevail.
the fundamental rights of the data subject over the legitimate interests of the controller or third party. Thus, consent may be considered a more appropriate legal hypothesis for the use of advertising cookies, subject to the applicable legal requirements and the circumstances of the particular case. This conclusion is reinforced when considering that advertising cookies are classified as non-necessary and that it is of paramount importance to respect the legitimate expectations of data subjects, giving them greater control over the use of their personal data in the digital environment.

example 3

Legitimate interest in the use of necessary cookies.

A bookstore provides online sales of books on its website. To do so, it uses cookies to ensure proper user authentication, payment and storage of information about the items inserted in the shopping cart. In the cookie banner, the bookstore informs you that cookies are collected exclusively for these specific purposes; this information is also in the cookie policy.

Analysis - In this case, the cookies used are strictly necessary for the operation of the website, as they are related to essential elements of the *online* book selling service. The interest of the controller may be considered legitimate, insofar as it supports and promotes its activities by enabling the provision of services that benefit the data subject. Moreover, the use of personal data exclusively for these specific purposes, as stated in the *banner* and in the controller's *cookie* policy, meets the legitimate expectations of the data subjects.

example 4

Use of cookies for audience measurement.

A cultural center of a municipality, constituted as a franchise, decided to adopt cookies on its website, for the specific purpose of obtaining visitation statistics and the performance of certain functionalities of the site. After internal evaluation, the authority concluded that the collection of data by means of the cookies in question could be carried out based on its legitimate interest, considering the limitation of the collection to what is strictly necessary for the specific and exclusive purpose of measuring the audience of the website, as described above. The data collected is also aggregated for the purpose of producing anonymous statistics. This information is not shared with third parties and is not cross-referenced with other databases to achieve other purposes. The explanation about the use of these cookies, their purposes and respective retention periods, as well as the possibility of opposing the treatment, is presented to the holder in the banner and in the cookies policy.

Analysis - The processing of data based on the legitimate interest of the autarchy is compatible with the LGPD, since, in this case, the collection of the data is not legally compulsory and there is no link

clear and direct between its specific purpose and the exercise of a typical state prerogative. It is therefore possible to weigh the interests of the municipality against the rights and legitimate expectations of the data subjects. The fact that the data collected are intended exclusively to produce visitation statistics, that they are not shared with third parties or combined with other information, and that information is presented in accordance with the principle of transparency, are elements that reinforce the legitimacy of the authority's interest in carrying out the processing and that indicate that the impact on the rights of the data subjects will be reduced.

Cookie Policies

To comply with the principle of transparency and to help the holder to com- 28

In order to understand the handling of personal data collected through *cookies*, it is recommended that a *Cookie Policy* or equivalent document - i.e. a public statement that makes information available to users of a website or application - be developed. In compliance with the principles of free access and transparency, the *Cookies* Policy should present information on the specific purposes that justify the collection of personal data through cookies, the retention period and whether there is sharing with third parties, among other aspects indicated in article 9 of the Igpd.

It is important to differentiate between *Cookie* Policy and *Cookie Banner*. A *cookie banner* is a visual feature used in the *design of* applications or websites that uses prominent reading bars to inform the data subject in a brief, simple and direct manner of the use of *cookies* in that environment. In addition, the *banner* provides tools for the user to have greater control over the treatment, such as allowing them to consent or not to certain types of *cookies*. There are many ways to design a *Cookie Banner*, and best practices such as *User Experience*, or ux, *design* techniques generally align with Igpd's principles and obligations for handling personal data.

In turn, the Cookies Policy is usually available on a specific page, which contains more detailed information on the subject, and can generally be accessed through a *link in* the *banner*. It may also be integrated, in a prominent and easily accessible way, with the Privacy Notice (or "Privacy Policy") - the public statement of the data controller on the processing of personal data in general. In some cases, the data controller prefers to bring its *Cookie* Policy diluted in the *cookie banner*, i.e. the set of information about the use of *cookies* appears in the various layers of the *banner*.

Provided that the essential information is presented to the holder, 29
All these options are legitimate, so that the *Cookies* Policy can be presented: (i) as a specific section of the Privacy Notice; (ii) in a specific and separate location; or (iii) in the *cookies banner* itself. In other words, regardless of the mechanism adopted, what is important is that clear, accurate and easily accessible information is made available on the use of *cookies* and the collection of personal data when the owner accesses a given website, service or application, in compliance with the principles of transparency and free access and with article 9 of the lgpd.

Cookie Banners

Cookie banners are widespread mechanisms in the digital environment, developed as a way to materialize the principles set forth in the lgpd, especially those of transparency and free access. By presenting essential information on the use of cookies in a summarized and simplified manner, the *banners* contribute to the process of conscious decision making by the holder, in addition to strengthening control over their personal data and respect for their legitimate expectations. Thus, the *banner* serves as a tool to bring transparency and adherence to the principles of personal data protection.

In this sense, the present topic will present non-exhaustive guidelines, considered as good practices, in order to assist the treatment agents in designing *cookie banners* in a manner compatible with the provisions of the lgpd.

What to watch out for in the elaboration

top-level banners

- Provide an easily visible button to reject all unneeded *cookies* on the first and second level *banners.*

- Provide an easily accessible *link* for the data subject to exercise their rights, which may include, for example, learning more about how their data is used and the retention period, as well as requesting deletion of data, objecting to processing, or revoking consent.

second level banners

- Sort the *cookies* into categories in the second level *banner;*
- Describe the categories of *cookies according to* their uses and purposes;
- Provide simple, clear and precise description and information regarding these purposes;
- Allow consent to be obtained for each specific purpose, according to the categories identified in the second level *banner*, where appropriate;
- Disable consent-based cookies by default.

- Provide information on how to block *cookies* through the browser settings. If the *cookie* or tracker cannot be disabled through the browser, the owner must be informed about it.

What to avoid when designing cookie banners

The following describes inadvisable practices when designing cookie banners on websites.

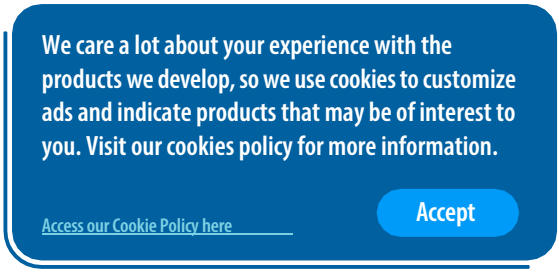
- Use a single button on the first level *banner*, with no management option in the case of using the legal hypothesis of consent ("I agree", "I accept", "I am aware", etc.);
- Make it harder to see or understand the buttons for rejecting *cookies* or setting *cookies*, and make only the accept button more prominent;
- Make it impossible or difficult to reject all non-neo- 33 *cookies* cessary;
- Display *cookies* not required enabled by default, requiring manual deactivation by the owner;
- Do not provide second level *banner*;
- Failure to provide information and direct, simplified and proper mechanism for the exercise of the rights of revocation of consent and objection to processing by the data subject (in addition to browser blocking settings);
- Make it difficult to manage *cookies* (e.g., not providing specific management options for *cookies* that serve different purposes);
- Display *cookie* policy information in a foreign language only;
- Present a list of *cookies* that is too granular, generating an excessive amount of information, which makes it difficult to understand and can lead to a fatigue effect, not allowing the holder to express his will in a clear and positive way;
- When using consent as a legal hypothesis, link its obtaining to the full acceptance of the conditions of use of *cookies*, without providing effective options to the holder.

Examples of cookie banners

example 5

Cookie Banner (first level)

Delta, in order to ensure compliance of its cookie practices with data protection legislation, has updated its website by inserting the following cookie banner on the home page:

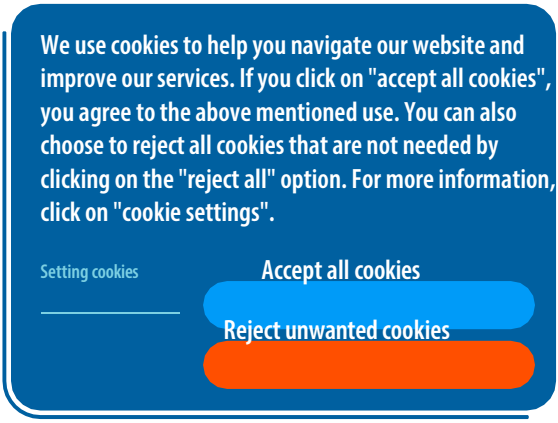


Analysis - In the example, the *banner* outlines the purposes of *cookie* handling and provides a link to the *cookie* policy of the *website*. However, it is only possible to see an "Accept" button, so that it is not possible to ensure clear manifestation of consent to the treatment, under the terms of the lgpd. Therefore, the *banner* should be adjusted by including an option for: (i) rejection of unnecessary *cookies*; and (ii) management of *cookies* through a second level *banner.*

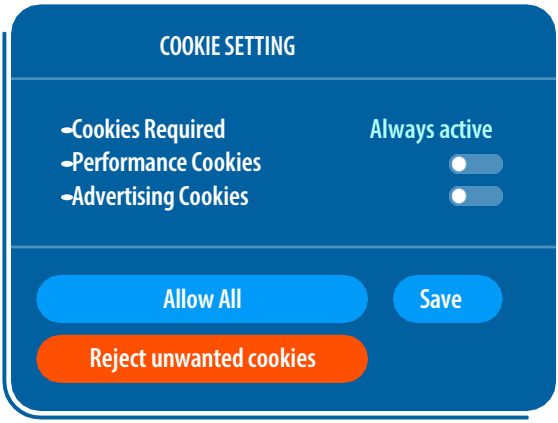
example 6

Cookie Banners (first and second level)

The Alpha company, when updating its website, inserted a cookie banner containing the following text:



An Alpha customer accesses the website and encounters such a banner on the first level. Since the customer does not want to accept or refuse all cookies, he clicks on the option "cookie settings", which takes him to a second-level banner, where he can see more detailed information.



In this second banner, cookies are grouped into categories: ne- cessary, performance, and advertising. With the exception of the first

category, the others are disabled by default. Specific consent can be obtained for each category, with the exception of the first category, which are cookies required for navigation. In addition, the "Reject Cookies Not Required" button remains highlighted.

Analysis - In the example above, consistent with lgpd provisions on consent, the *cookies banner* at the first level, unlike in example 5, has a button to reject all *cookies*. Also compliant with lgpd, there is a second level *banner* that allows for specific consent to be obtained according to the categories of consent.
gories identified. Another positive point refers to the deactivation by default from *cookies that are* not required, ensuring that a positive response is obtained from the data subject.

example 7

Cookie Policy next to Privacy Policy

José, an accountant, in creating his accounting office's website, has chosen to make the Cookie Policy available next to the Privacy Policy.

Analysis - This practice can be legitimately adopted, preferably by providing easy access to the *cookie* policy section. For example, access could be facilitated through a tab, sidebar or summary at the beginning of the Privacy Policy. However, providing information about *cookies* only through the Privacy Policy may not be sufficient as a data subject will not always refer to a *website*'s Privacy Policy page. Therefore, it is recommended that features be provided so that the data subject can identify such information separately upon accessing the platform, such as through the use of a second level banner.

Final considerations

The present Guide is designed to provide guidance to treatment agents on how to deal with the - 37
to the best practices related to the treatment of personal data resulting from the collection of *cookies*. To this end, we sought to bring the concept of *cookies*, some categories into which they can be classified, and their purposes. In addition, the main provisions of the GDPR applicable to the collection of personal data through *cookies* were listed. Guidelines were also presented on the development of *Cookie* Policies and *cookie banners*, by means of illustrative examples.

Finally, we emphasize that this document may be adapted to future regulations on the topics listed here and should be understood as a guide to best practices, which can be updated and improved whenever necessary.

Notes

Concept and classifications ▶ p. 8-12

[1] Other possible definitions can be found in: HOOFNAGLE, et al. *Behavio- ral Advertising: The Offer You Cannot Refuse*. Harvard Law & Policy Review, vol.6, n. 273, 2012. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601 and KRISTOL, David.M. HTTP *Cookies: Standards, Privacy, and Politics*. ACM Transactions on Internet Technology, Vol. 1, No. 2, 2001. Available at: https://dl.acm.org/doi/pdf/10.1145/502152.502153. ▶ p.8

[According to art. 12, § 2º, of the lgpd: "Art. 12.

personal data, for the purposes of this Law, those used for profiling 38
behavior of a particular natural person, if identified." ▶ p.9

Cookies and the LGPD ▶ p. 13-27

[3] The matter is regulated by art. 10 of the MCI, which reserves the possibility of access to registration data by competent administrative authorities. Similarly, clauses ii and iii of art. 7 ensure the inviolability and confidentiality of the flow of private communications over the Internet, including stored private communications, "except by judicial order". ▶ p.14

[4] The guidance presented here on the legal bases of consent and legitimate interest follows, with adaptations, that set out in the Guidance - *Application of lgpd by treatment agents in the electoral context*, p. 21-25; and 27-29. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf. ▶ p.17

[5] It is worth emphasizing that "consent may eventually be admitted as a legal basis for the treatment of personal data by the Public Power. For this purpose, the use of the data should not be compulsory and the state action should not, as a rule, be based on the exercise of typical state prerogatives, which derive from the fulfillment of legal obligations and attributions". *Guia Orientativo - Tratamento de dados pessoais pelo Poder Público*, jan. 2022, p. 7. Available at: https://www.gov.br/anpd/pt-br/documentos--e-publications/guide-public-power-anpd-version-final.pdf. ▶ p.20

[6] It is worth emphasizing that "the legitimate interest may eventually be admitted as a legal basis for the processing of personal data by the Public Authorities. To this end, the uti-

data use should not be compulsory or, furthermore, state action should not be based on the exercise of typical state prerogatives, which derive from the fulfillment of legal obligations and attributions. In this context, it becomes effectively possible to carry out a balancing between, on the one hand, the legitimate interests of the controller or third party and, on the other, the legitimate expectations and rights of the data subjects." *Guia Orientativo - Tratamento de dados pessoais pelo Poder Público*, jan. 2022, p. 8. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. ▶ p.24

ANPD

Autoridade Nacional de Proteção de Dados

www.anpd.gov.br

@anpdgov