Eleven Paths

Telefónica CYBER SECURITY COMPANY

Is the Oven Ready for Cookies?

Analysis of the Regulatory Compliance of Cookies in Spain

Introduction

Every time we visit a website, we are asked whether we want to accept or (almost always indirectly) refuse cookies. Most users who arrive at this message looking for a service or specific information end up accepting all cookies without knowing the real impact in terms of security and privacy.

How many cookies are usually accepted? For how long? Do the websites respect the new law on cookies?

In TEGRA, the information protection innovation centre of the ElevenPaths innovation area and laboratory in Galicia, we wanted to analyse the current use of cookies in Spain and their impact and compliance based on a representative sample of the most visited websites in Spain.

To achieve this we have developed and released a tool called Triki, which automates the navigation to a series of websites defined by configuration and performs different navigation flows: visit, acceptance and rejection by extracting the cookies stored in each flow and creating statistics on them.

Before going deeper into our analysis, it is useful to be clear about some concepts on cookies, those small data files that websites send to browsers. Browsers store these files and return them the next time they are visited.

The **Agencia Española de Protección de Datos** (Spanish Data Protection Agency) classifies cookies according to a series of non-exclusive categories.

Types of Cookies According to Their Purpose

- **Technical cookies:** those that allow the user to browse through a website, platform or application and use the different options or services that in it exists, including those that the publisher uses to enable the management and operation of the website and to enable its functions and services. Such as, for example, controlling data traffic and communication, identifying the session, accessing parts of restricted access, ... Also belonging to this category, due to their technical nature, are those cookies that allow the management of advertising spaces.
- **Preference or personalisation cookies:** these allow information to be remembered so that the user can access the service with certain characteristics that can differentiate their experience from that of other users, such as, for example, the language, the number of results to be shown when the user carries out a search, the appearance or content of the service depending on the type of browser, etc.
- **Analysis or monitoring cookies:** these allow the monitoring and analysis of the behaviour of the users of the websites to which they are linked, including the quantification of the impacts of the advertisements.
- **Behavioural advertising cookies:** are those that store information on the behaviour of users obtained through continuous observation of their browsing habits, which allows the development of a specific profile to display advertising based on it.

Types of Cookies According to the Entity that Manages Them

- **Own cookies:** those that are sent to the user's terminal equipment from a computer or domain managed by the editor of that website and from which the service requested by the user is provided.
- **Third-party cookies:** those that are sent to the user's terminal equipment from a computer or domain that is not managed by the editor, but by another entity that processes the data obtained through cookies.

Types of Cookies According to the Lenght of Time They Remain Activated

- **Session cookies:** are those designed to collect and store data while the user accesses a website. They are usually used to store information that is only interesting to keep for the provision of the service requested by the user on one occasion (for example, a list of products purchased) and they disappear at the end of the session.
- **Permanent cookies:** are those in which the data is still stored in the terminal and can be accessed and processed during a period defined by the person responsible for the cookie, which can range from a few minutes to several years.

Cookies and Consents

Every time you visit a website, we are asked for consent. **But when is consent necessary?** When the use of a cookie involves the processing of personal data, as explained in the previous section, data controllers must ensure compliance with the additional requirements established by the regulations on the protection of personal data, in particular with regard to special categories of data. **Processing of personal data shall be deemed to exist when the user is identified by a name or email address of that identifies it (e.g. because it is a registered user)** or where unique identifiers are used to distinguish between users and to track them individually (e.g. an advertising ID).

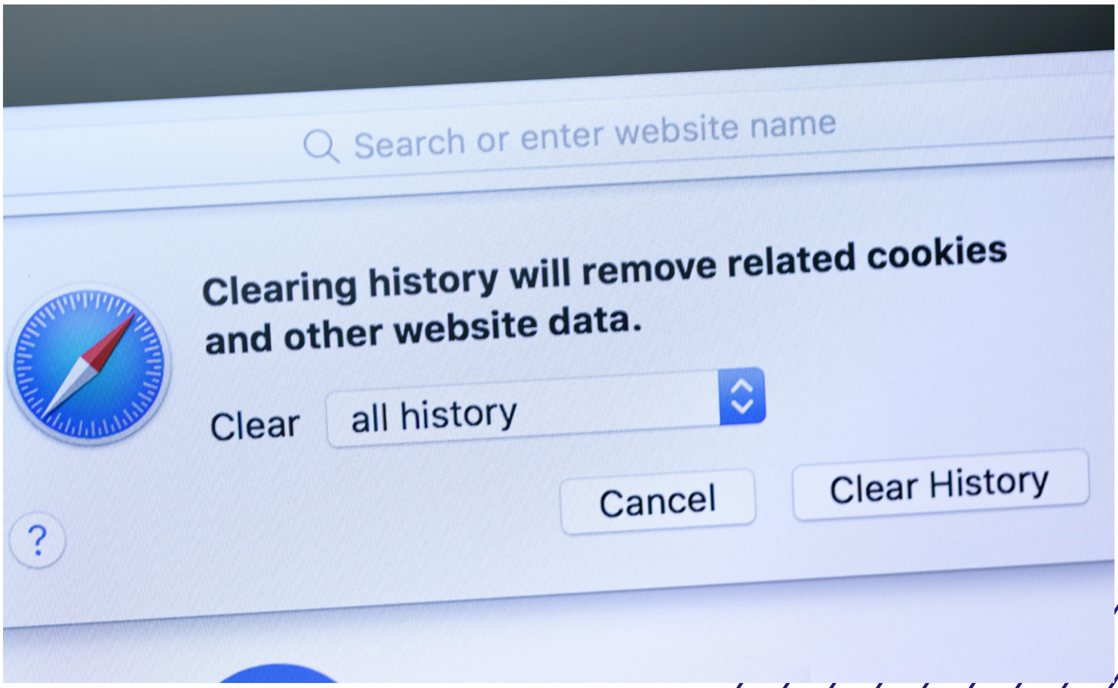
In general, cookies used for any of the following purposes are exempt from the obligations established in the 22.2 article of the LSSI:

- Allow only communication between the user's equipment and the network.
- Strictly provide a service expressly requested by the user.

In this regard, the GT29, in its 4/201210 judgment, interpreted that among the exempted cookies would be those that have as their purpose:

- **User input cookies.** Session and user input cookies are typically used to track user actions when filling out online forms on various pages or as a shopping cart to keep track of items the user has selected at the click of a button.
- **Authentication or user identification cookies (session only).**
- **User security cookies.** For example, cookies used to detect repeated and unsuccessful attempts to connect to a website.
- **Media player session cookies.**
- **Session cookies for load balancing.**
- **User interface personalisation cookies.** The exception only applies to users who have decided to keep the session open.
- **Certain plug-in cookies** for exchanging social content.

These types of cookies are known as technical cookies and/or personalisation cookies, and are excluded from the scope of the application, which means that it would not be necessary to inform about them or obtain consent. In other words, on sites where only these types of cookies are used, it is not necessary to inform the user that they are being used or to request consent for its use. However, for reasons of transparency, it is recommended to report on them, at least on a generic basis.



Clearing history will remove related cookies and other website data.

The Reason to Legislate

Cookies are not dangerous themselves. They cannot infect devices with malware on their own, for example. However, if stolen by third parties, they could allow access to different services such as: the email account, the social network or the shop where we make our purchases. This applies to security cookies, whether they are session or permanent cookies.

In addition, there are other types of cookies, known as ***third-party cookies***, which can have a strong impact on our privacy. According to the AEPD's (Spanish Data Protection Agency) Guide to the Use of Cookies:

"Individuals can be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, session identifiers in the form of «cookies» or other identifiers, such as radio frequency identification tags.

This can leave traces that, in particular, when combined with unique identifiers and other data received by the servers, can be used to profile and identify individuals".

This type of cookie is usually associated with behavioural advertising cookies, since they store information on the behaviour of users obtained through continuous monitoring of their browsing habits, which allows the development of a specific profile to display advertising based on this. **These are the typical cookies with which a seller "chases" you on other sites that share product advertising you have searched for on another website.**

On the other hand, ***analysis or monitoring cookies*** allow the person responsible for them to track and analyse the behaviour of the users of the websites to which they are linked. Although they are not exempt from the duty to obtain informed consent for their use, they are less likely to represent a risk to the privacy of users provided that they are their ***own cookies*** (or first party cookies), which process aggregate data for a strictly statistical purposes.

These cookies are not essential as far as navigation is concerned. Nor do they allow access to our accounts, but they do have some impact on our privacy, since, as mentioned above, they can be used to identify or profile users, collect information about our tastes, browsing habits, searches and how we spend our time. **This allows advertising or analytics companies to track the user's browsing history on all websites that use their ads.**

All this information is used to show us personalised advertising or to carry out market research. These are among the cookies that require the most attention.

New Regulations In the AEPD 2020 Cookie Guide

In collaboration with Govertis, we will explain what has happened in 2020 concerning cookies and their management. The Spanish Data Protection Agency (AEPD), following the entry into force of the European General Data Protection Regulation and several consultations with the European Data Protection Supervisor (EDPS), updated its guide to the use of cookies in July 2020, giving website owners a deadline to adapt to these policies until 31 October 2020.

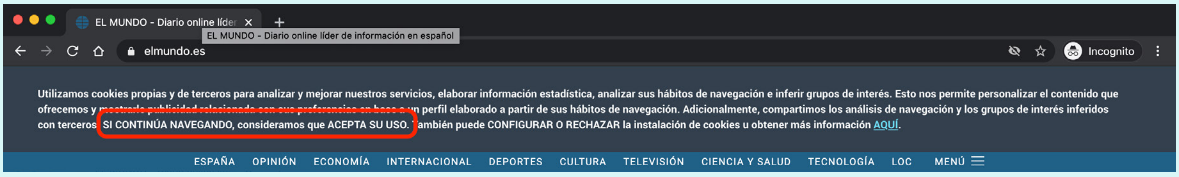
We could summarise the main changes in:

- Simple navigation is not valid as an expression of a user's consent to the acceptance of cookies.
- Strengthening the regulation on cookie walls.
- Developments in the management of acceptance and revocation of consent.

The removal of the option to obtain consent through the "continue browsing" option.

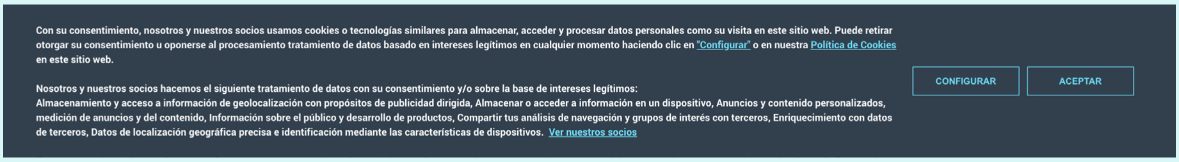
- Previously, the following option was allowed: "If you continue to browse, we consider that you accept its use".
- Now: "The EDPS has established that continuing to sail is not a valid way of giving consent".

Many IT departments have been busy carrying out this task of adaptation to comply with the new regulations, for example, we can see the change in the informative text of the cookies on the website of the newspaper **El Mundo**:



Utilizamos cookies propias y de terceros para analizar y mejorar nuestros servicios, elaborar información estadística, analizar sus hábitos de navegación e inferir grupos de interés. Esto nos permite personalizar el contenido que ofrecemos y mostrarle publicidad relacionada con sus preferencias en base a un perfil elaborado a partir de sus hábitos de navegación. Adicionalmente, compartimos los análisis de navegación y los grupos de interés inferidos con terceros. SI CONTINÚA NAVEGANDO, consideramos que ACEPTA SU USO. También puede CONFIGURAR O RECHAZAR la instalación de cookies u obtener más información AQUÍ.

Before 31 October 2020



Con su consentimiento, nosotros y nuestros socios usamos cookies o tecnologías similares para almacenar, acceder y procesar datos personales como su visita en este sitio web. Puede retirar otorgar su consentimiento u oponerse al procesamiento tratamiento de datos basado en intereses legítimos en cualquier momento haciendo clic en "Configurar" o en nuestra Política de Cookies en este sitio web.

Nosotros y nuestros socios hacemos el siguiente tratamiento de datos con su consentimiento y/o sobre la base de intereses legítimos:
Almacenamiento y acceso a información de geolocalización con propósitos de publicidad dirigida, Almacenar o acceder a información en un dispositivo, Anuncios y contenido personalizados, medición de anuncios y del contenido, Información sobre el público y desarrollo de productos, Compartir tus análisis de navegación y grupos de interés con terceros, Enriquecimiento con datos de terceros, Datos de localización geográfica precisa e identificación mediante las características de dispositivos. Ver nuestros socios

After the entry into force of AEPD's new regulations

The prohibition of the use of cookie walls, if no alternative to consent is offered.

- **It is not allowed:** in those cases in which the denial of access would prevent the exercise of a legally recognised right of the user, for example, access to a website is the only means provided to the user to exercise such a right.
- **It is allowed:** when the non-acceptance of the use of cookies prevents access to the website or the total or partial use of the service, provided that:
  - › the user is properly informed,
  - › an alternative access to the service is offered without the need to accept the use of cookies,
  - › the services of both alternatives must be genuinely equivalent and, also, it will not be valid that the equivalent service is offered by an entity external to the publisher.

New requirements for making a cookie wall have been outlined in italics.

Some aspects relating to the methods for informing users about the acceptance, refusal or revocation of consent are modified and clarified, through the configuration.

- As a general rule:
  - › Through the functionalities provided by the editor (the cookie management or configuration system that has been enabled).
  - › Through the common platforms that may exist for this purpose.
- If the management system or configuration of the editor's cookies does not allow the use of ***third-party cookies*** to be avoided once they have been accepted by the user:
  - › Information will be provided about the tools provided by the browser and third parties and
  - › it should be noted that if the user accepts ***third party cookies*** and subsequently wishes to delete them, this should be done from their own browser or the system enabled by the third-party.

Our Analysis, What Do Cookies Really Do?

To carry out this research on cookies, the 100 most visited domains in Spain have been selected, obtained through the alexa.com website. To extract the information, a tool called Triki has been developed, programmed in Python, and its description is included at the end of the article.

Using the Triki tool and a personalised configuration per domain, different types of information have been extracted, grouped in two types of tables: cookies and stats. Both tables make up our dataset.

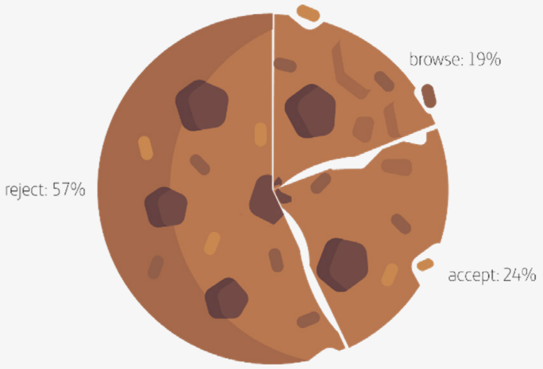
Each website has been monitored based on a series of flows. In addition, for each flow, two types of extraction have been performed: extraction without blocker and extraction using a third-party cookie blocker.

The different flows simulated with each type of browsing are:

- **browse:** the tool connects to the website without taking any action and extracts the cookies used. It is the part before the consent of the cookies.
- **accept:** the tool connects to the website, consents to the use of all cookies and extracts them. This is the acceptance part of cookies.
- **reject:** the connection to the website is made and the necessary actions are taken to proceed with the rejection of the cookies. This is the part that rejects cookies.

Not all the websites selected allow for acceptance or rejection. It is possible that a website does not notify or request the acceptance of cookies as long as it only uses technical cookies or personalisation cookies, although the AEPD recommends that the user be notified for transparency reasons.

How many domains does each flow allow?



- 19 websites only allow browsing (browse), without allowing to reject or accept cookies.
- 24 websites allow you to browse the site and accept cookies (accept).
- 57 websites allow you to browse, accept and reject cookies (reject).

This means that more than 50% of the pages in our survey allow the rejection or configuration of cookies directly. 24% allow only acceptance and redirect the user to the browser's own configuration for rejection, which increases the effort to perform the rejection. 19 of them (19%) do not allow to reject or accept, but they could be pages without cookies that must be notified. Of these, 9 (37%) use analytical cookies (Google Analytics) and therefore do not comply with the need for express consent expressed by the regulation of cookies of the AEPD.

The Difficulty of Rejection

Let's not fool ourselves, many sites do not want us to reject cookies. But they must comply with the law, so they offer this possibility, but in a somewhat more complex way for the user. Examples of good practice in requesting user consent are shown in the Guide to the Use of Cookies. One of these, the simplest and most transparent, is to allow all cookies to be rejected from the usage information panel itself. Of the domains analysed that allow the rejection of cookies through the page, only 8% of the web pages allow rejection directly from the warning banner.

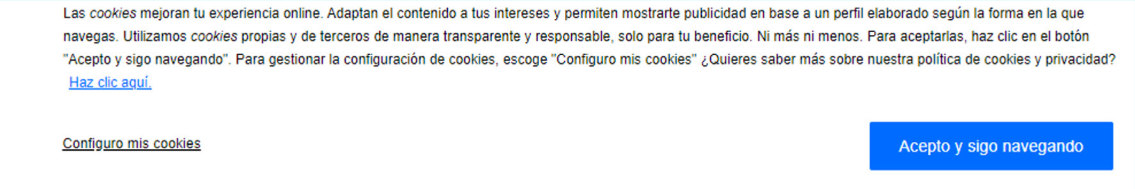
In the case of sites that use a second layer, where it is necessary to enter the configuration, the guide indicates that there is a button that allows all cookies to be rejected without further interaction by the end user. Of the pages analysed, 70% comply with this premise.

The remaining 22% do not comply with the regulations in force or with the requirement mentioned above. Between 3 and 5 actions (clicks) are necessary to be able to totally reject the cookies. The most common reasons are that panels are added prior to rejection or that it is necessary to disable cookies one by one.

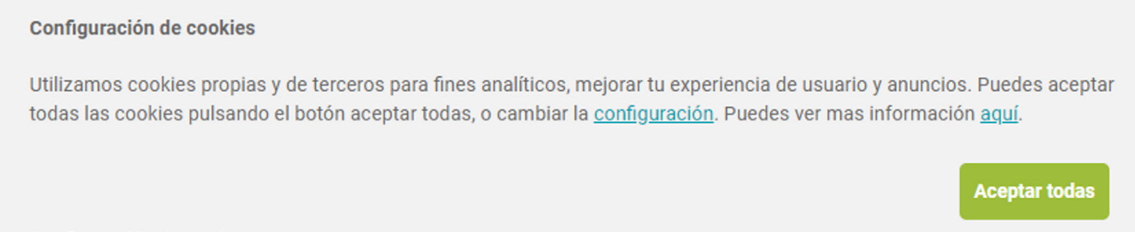
Bias for Accepting Cookies

We have already mentioned that when deciding whether to consent to cookies it is easier to accept than to reject. Different methods are used which, without being illegal, may result in unorthodox techniques that do not comply with or at least violate the spirit of the requirement conveyed by the AEPD: "that it be as easy to withdraw consent as to give it".

Here are some warning panels about the use of cookies:



Las *cookies* mejoran tu experiencia online. Adaptan el contenido a tus intereses y permiten mostrarte publicidad en base a un perfil elaborado según la forma en la que navegas. Utilizamos *cookies* propias y de terceros de manera transparente y responsable, solo para tu beneficio. Ni más ni menos. Para aceptarlas, haz clic en el botón "Acepto y sigo navegando". Para gestionar la configuración de cookies, escoge "Configuro mis cookies" ¿Quieres saber más sobre nuestra política de cookies y privacidad? Haz clic aquí.



Configuración de cookies

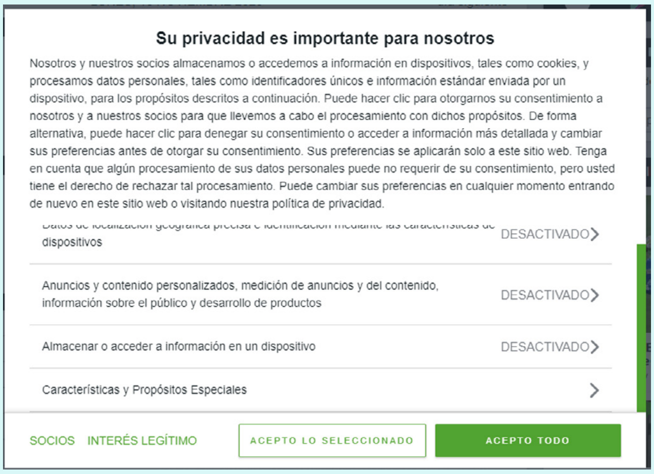
Utilizamos cookies propias y de terceros para fines analíticos, mejorar tu experiencia de usuario y anuncios. Puedes aceptar todas las cookies pulsando el botón aceptar todas, o cambiar la configuración. Puedes ver mas información aquí.

The panels shown as examples are totally legal and comply with the current regulations set out in the AEPD's Guide to the Use of Cookies. However, **the word "reject" is not explicitly mentioned (only the configuration is mentioned) which implies that the user must pay more attention to know how to proceed with the rejection.** On the contrary, the button to accept stands out above everything else, which is easier for the user and means less effort to get rid of the information banner that disturbs or makes navigation impossible.

The very fact of having to reject cookies means that the user no longer pays attention to what he or she was looking for in the content of the website, but rather focuses on how to reject the cookies. **This feeling of added effort can generate a frustration that makes it easier to decide to accept cookies rather than reject them so as not to deviate from the main objective of visiting that website.**

These types of " acceptance by fatigue " techniques are also used in the configuration or rejection panels

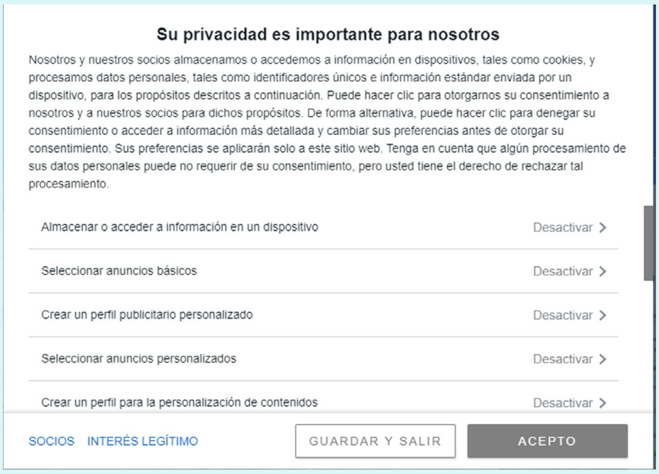
Here are some examples:



Su privacidad es importante para nosotros

Nosotros y nuestros socios almacenamos o accedemos a información en dispositivos, tales como cookies, y procesamos datos personales, tales como identificadores únicos e información estándar enviada por un dispositivo, para los propósitos descritos a continuación. Puede hacer clic para otorgarnos su consentimiento a nosotros y a nuestros socios para que llevemos a cabo el procesamiento con dichos propósitos. De forma alternativa, puede hacer clic para denegar su consentimiento o acceder a información más detallada y cambiar sus preferencias antes de otorgar su consentimiento. Sus preferencias se aplicarán solo a este sitio web. Tenga en cuenta que algún procesamiento de sus datos personales puede no requerir de su consentimiento, pero usted tiene el derecho de rechazar tal procesamiento. Puede cambiar sus preferencias en cualquier momento entrando de nuevo en este sitio web o visitando nuestra política de privacidad.

Datos de localización geográfica precisa e identificación mediante las características de dispositivos	DESACTIVADO
Anuncios y contenido personalizados, medición de anuncios y del contenido, información sobre el público y desarrollo de productos	DESACTIVADO
Almacenar o acceder a información en un dispositivo	DESACTIVADO
Características y Propósitos Especiales	



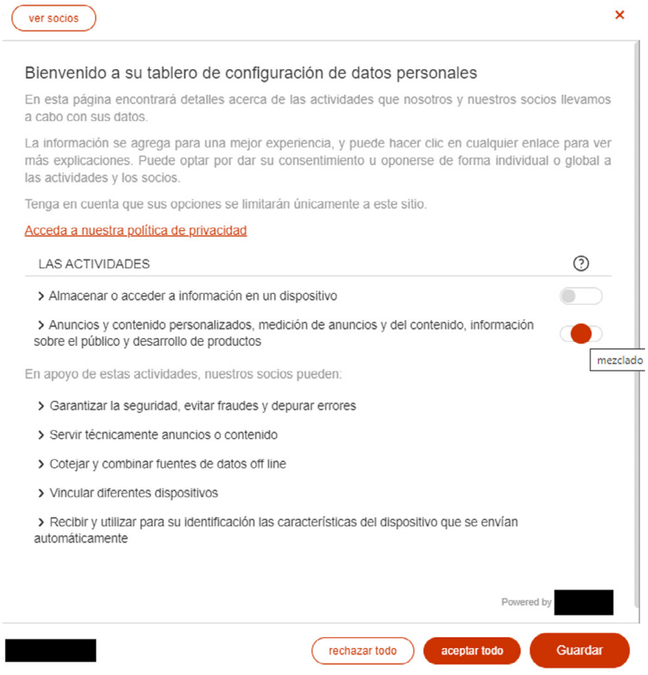
Su privacidad es importante para nosotros

Nosotros y nuestros socios almacenamos o accedemos a información en dispositivos, tales como cookies, y procesamos datos personales, tales como identificadores únicos e información estándar enviada por un dispositivo, para los propósitos descritos a continuación. Puede hacer clic para otorgarnos su consentimiento a nosotros y a nuestros socios para dichos propósitos. De forma alternativa, puede hacer clic para denegar su consentimiento o acceder a información más detallada y cambiar sus preferencias antes de otorgar su consentimiento. Sus preferencias se aplicarán solo a este sitio web. Tenga en cuenta que algún procesamiento de sus datos personales puede no requerir de su consentimiento, pero usted tiene el derecho de rechazar tal procesamiento.

Almacenar o acceder a información en un dispositivo	Desactivar
Seleccionar anuncios básicos	Desactivar
Crear un perfil publicitario personalizado	Desactivar
Seleccionar anuncios personalizados	Desactivar
Crear un perfil para la personalización de contenidos	Desactivar

Again, no regulations are being violated and these are recommended examples. What is striking is the way in which the buttons are represented, highlighting those of acceptance versus those of rejection or even pretending that they are not active.

In many cases, the names of the buttons tend to be ambiguous and induce to accept the cookies even if they think they are being rejected.



Bienvenido a su tablero de configuración de datos personales

En esta página encontrará detalles acerca de las actividades que nosotros y nuestros socios llevamos a cabo con sus datos.

La información se agrega para una mejor experiencia, y puede hacer clic en cualquier enlace para ver más explicaciones. Puede optar por dar su consentimiento u oponerse de forma individual o global a las actividades y los socios.

Tenga en cuenta que sus opciones se limitarán únicamente a este sitio.

Acceda a nuestra política de privacidad

LAS ACTIVIDADES

- Almacenar o acceder a información en un dispositivo ○
- Anuncios y contenido personalizados, medición de anuncios y del contenido, información sobre el público y desarrollo de productos ● mezclado

En apoyo de estas actividades, nuestros socios pueden:

- Garantizar la seguridad, evitar fraudes y depurar errores
- Servir técnicamente anuncios o contenido
- Cotejar y combinar fuentes de datos off line
- Vincular diferentes dispositivos
- Recibir y utilizar para su identificación las características del dispositivo que se envían automáticamente

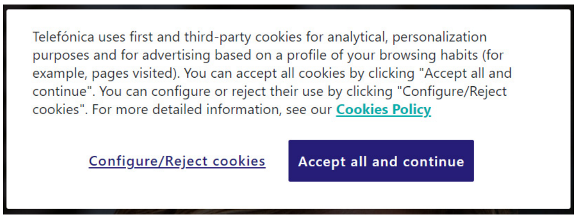
Powered by [redacted]

[redacted]

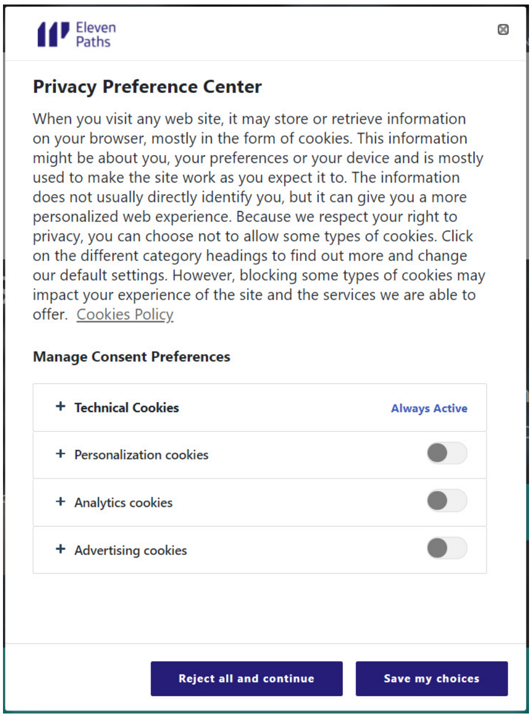
In the example of the image you can see that if you don't keep the mouse pointer over the element it doesn't get bigger and the mixing caption doesn't appear.

In general, in this type of configuration panels, different digital marketing techniques are being used (well known in many other areas) that cause the user to focus on the interest of the page itself: accepting cookies.

In contrast, **there are warning panels that allow you to accept and reject cookies at the touch of a button without making any distinction.** Similarly, there are settings panels that clearly allow you to accept, reject or adjust a personalised configuration, as shown below:



Telefónica uses first and third-party cookies for analytical, personalization purposes and for advertising based on a profile of your browsing habits (for example, pages visited). You can accept all cookies by clicking "Accept all and continue". You can configure or reject their use by clicking "Configure/Reject cookies". For more detailed information, see our **Cookies Policy**



Privacy Preference Center

When you visit any web site, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer. Cookies Policy

Manage Consent Preferences

+ **Technical Cookies** Always Active
+ Personalization cookies ○
+ Analytics cookies ○
+ Advertising cookies ○

Installation of Cookies Before Consent

As mentioned above, under current regulations, with the exception of ***technical*** or ***personalisation*** cookies, these should not be used without prior acceptance or rejection.

Therefore, we have made **an analysis of the cookies that are established just by visiting a website, prior to consent.** The results obtained from our analysis are as follows:

- 53% of websites use more than 10 cookies before consent.
- By using a ***third-party cookie*** blocker in the browser, it is shown that 96% of sites use third-party cookies right after login. While this may be legal, it is at least rare that they require cookies of third parties to ensure the technical operation or customization of a page.
- Using a ***third-party cookie*** blocker greatly helps to remove a lot of unnecessary cookies.

Accepting Cookies

As we mentioned at the beginning of this article, when accepting cookies from a certain site we could be accepting a large number of different types of cookies as the data shows:

- 14% use more than 90 cookies.
- The average use of cookies corresponds to 27 cookies per website.

We now compare ***own cookies*** with ***third-party cookies*** in our entire dataset.

- 44% of websites use the same or more third-party cookies than their ***own cookies***.
- In the most unfavourable cases, 90% of a website's cookies are ***third-party cookies***.

Rejecting Cookies

Analysing the difference between acceptance and rejection of cookies, in our analysis we have observed that when cookies are rejected their number decreases by 46% compared to when they are accepted.

On the other hand, we assume that the difference between an implicit consent based on mere browsing of the website and an explicit rejection of all cookies should result in a very similar number of cookies being set. **In our analysis we have found that 72% of the websites visited comply with this assumption.**

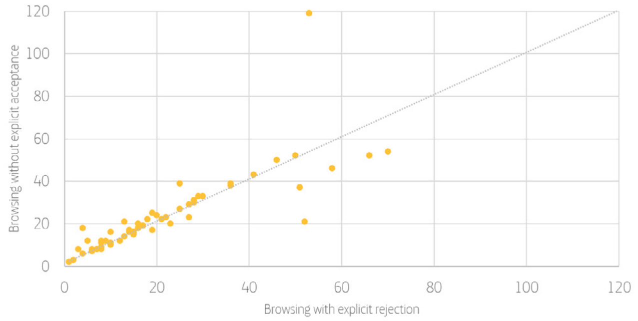
However, something that calls our attention is that we observe that 14% of the analysed sites show a difference of more than 5 cookies between rejection and simple browsing. **If we have refused to install all the cookies except those necessary for the technical functioning of the site, why do we have more cookies than when simply browsing?**

Other relevant information is that the remaining 14%, within our analysis universe, **have a lower number of cookies** after express rejection than after merely browsing the site. Simple browsing should not serve to establish more cookies in the client and, therefore, should be equivalent to explicit rejection, which could denote a breach of regulations in the initial browsing stage.

The following graph shows the difference in the setting of cookies when browsing without explicit acceptance and when explicitly rejecting.

14% OF THE ANALYSED WEBSITES SHOW A DIFFERENCE OF MORE THAN 5 COOKIES BETWEEN REJECTION AND SIMPLE NAVIGATION

Cookie setting difference when browsing without explicit acceptance and with explicit rejection.



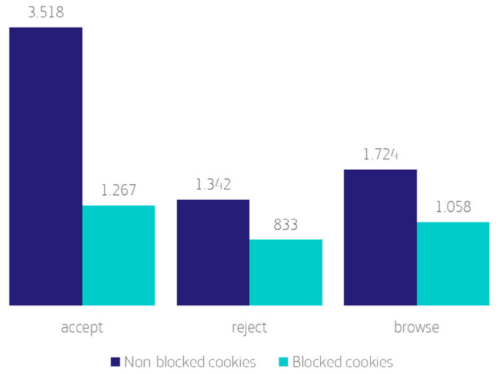
Blocking Third-Party Cookies

Cookies that we must pay special attention to are ***third-party cookies*** since they are the ones that have a strong impact on our privacy. Today's browsers often have systems in place to block third-party cookies. This [link] shows how to activate them in each browser and their main features. In some browsers this feature is enabled by default and in others it is necessary to enable it manually.

Below is the total number of cookies registered in all the domains, classified in stages, depending on whether or not third-party cookies have been blocked. Before consent, acceptance and rejection.

69% OF DOMAINS THAT ALLOW REJECTING THIRD-PARTY COOKIES DO NOT DELETE THEM COMPLETELY AFTER REJECTING

Total number of cookies registered in all domains sorted in stages, depending on whether or not third party cookies have been blocked



As can be seen from the results, the simple use of a third-party cookie blocker results in a significant decrease in the number of cookies used. Even if all cookies have been rejected.

We can conclude that 69% of the domains that allow you to reject cookies do not completely eliminate ***third-party cookies*** when you reject them with your browser.

Analytical Cookies

Under current regulations, analytical cookies require explicit consent from the user, so they cannot be used before that consent or, logically, after being rejected.

During our research we have analysed how many sites use Google Analytics cookies before accepting or refusing consent at the stage we have defined as "browse". The results show that **46% of the pages use Google Analytics cookies before consent.**

We also wanted to check how many sites still maintain **Google Analytics cookies** after an explicit rejection by the user. The results show that **25% of websites continue to keep this type of analytical cookie even when rejected.**

The browse and reject stages should show the same or very similar results, as explicit non-acceptance and rejection should show similar results. However, the evidence indicates otherwise.

The Importance of Session Cookies Versus Permanent Cookies

According to the AEPD's [Guide to the Use of Cookies](), the use of ***permanent cookies*** is indicated as follows:

"[...] it should be specifically assessed whether the use of permanent cookies is necessary, as the risks to privacy could be reduced by the use of session cookies".

To assess whether the websites are complying with this premise, permanent cookies have been compared with session cookies after accepting all cookies on the various websites.

The results show that:

- 96% of the websites analysed use more ***permanent cookies*** than ***session cookies***.
- On average, 86% of the total cookies used on a website are ***permanent cookies***.

In addition, the AEPD in its Guide on the Use of Cookies indicates that:

"In any case, when permanent cookies are installed, it is recommended that their temporary duration is reduced to the necessary minimum in accordance with the purpose of their use. To this end, GT29 4/2012 judgement indicated that for a cookie to be exempted from the duty of informed consent, its expiry must be related to its purpose. As a result, session cookies are much more likely to be exempted than permanent ones".

"The EDPS, in its guidelines on consent, recommends as best practice the renewal of consent at appropriate intervals. This Agency considers it good practice that the validity of users' consent to the use of a particular cookie should not be longer to 24 months and that during this time the selection made by the user on their preferences is kept, without being asked for a new consent each time they visit the website in question".

Based on these indications, we have analysed our dataset to verify whether the extracted cookies meet this requirement of a maximum life span of 24 months (2 years) for ***permanent cookies***.

The results are as follows:

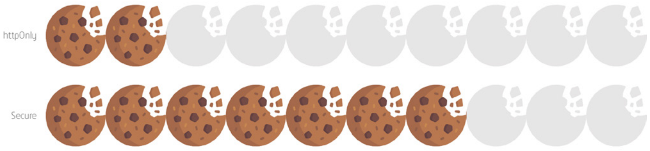
- **Around 15% of cookies violate this regulation by using expiration periods longer than 24 months.**
- When we accepted the cookies from the site visited, we found more than 100 cookies with a duration of more than 3 years. The expiration of 50 of these cookies is more than 20 years.

Securing Cookies

We also wanted to analyse which security systems are implemented in the established cookies themselves. Let's look at some of the methods analysed.

- **Secure cookies:** if this flag is enabled in the cookie, it would only be sent to the server in an encrypted HTTP request via the HTTPS protocol (HTTP + TLS/SSL).
- **HttpOnly cookies:** enabling this flag in a cookie helps prevent cross-site scripting (XSS) attacks, since HttpOnly cookies are inaccessible from the Javascript document.cookie API.

Below are the cookies detected with these flags activated from a sample of 3,694 total cookies:



- **Host and Secure prefixes:** cookie prefixes allow you to mark cookies so that they behave differently, in a way that is compatible with previous versions. To do this, a prefix is added to the name of the cookie that allows a flag to be set to that cookie. When the name of a cookie begins with a prefix, it activates an additional browsing policy on supported browsers. The ***__Secure-*** prefix makes a cookie accessible only from secure sites with the HTTPS protocol. This makes it impossible for an insecure site using the HTTP protocol to read or update cookies containing that prefix on its name. This security mechanism protects against attacks from tampering with secure cookies. The ***__Host-*** prefix does the same things as the __Secure- prefix, but at a higher level it restricts access only to the same domain in which it is configured. This means that a subdomain can no longer overwrite the cookie value.

After analysing all the cookies for these prefixes, we have found that:

- Only 2% of websites use the ***__Host-*** *prefix.*
- None of the websites use the ***__Secure-*** prefix.

Conclusions

- None of the websites that only uses technical cookies and/or personalisation cookies gives any kind of warning to the user that this type of cookie is being used. Although it is completely legal, the Guide to the Use of Cookies advises to make the warning as transparent as possible (this type of page usually belongs to state pages, non-profit organisations or pages with download content).
- **Only 8% of the websites analysed allow you to reject directly from the main banner.** Of the remaining percentage, 22% do not meet the premise that it is "as easy to reject as to accept", since more actions are needed to be able to disable the use of cookies. The remaining 70% who are compliant use marketing strategies to subtly induce the user to accept cookies. For example, with ambiguous buttons that make people think that cookies have been deactivated.
- The regulations indicate that as long as the user does not give his consent, cookies cannot be used, with the exception of technical and personalisation cookies. The results show that at least 10 cookies are being used on 53% of the websites analysed. Of the sites analysed, 96% use third party cookies as soon as they are connected, which is in violation of current regulations.
- As a first impression, you might think that most websites use more cookies of their own than those of third parties. The data indicates that 44% of the websites use the same or a greater number of ***third-party cookies*** than their ***own cookies***. In the worst cases, 90% of a website's cookies are ***third-party cookies***. In this case it is recommended to enable the blocking of the use of third-party cookies in the browser to limit the number of cookies. The results of the analysis show that, even if all cookies are rejected completely, many of these third-party cookies are still used in the same way.
- The regulations indicate that session cookies should be given priority over ***permanent cookies*** However, the data indicates that 96% of the sites analysed use more ***permanent cookies*** than ***session cookies***. In addition, on average, 86% of the total cookies used by a website are ***permanent cookies.*** The regulations indicate that the life span of these cookies should not exceed two years, however, 15% of the cookies use expiry periods of more than 24 months.
- There is a significant difference in the number of cookies installed between simply browsing the website and refusing cookies. 14% of the websites in our analysis have a difference of more than 5 cookies between the two " flows " when, logically, that difference should not be greater than one cookie to store the user's rejection.
- 46% of the websites use pre-consent analytical cookies and 25% use them when still refusing all cookies, so this is in violation of the AEPD policy.

TEGRA Cybersecurity Center is part of the joint research unit on cyber security IRMAS 2.0 (Information Rights Management Advanced Systems), which is co-financed by the European Union, within the framework of the ERDF Operational Programme Galicia 2014-2020, to promote technological development, innovation and quality research.

XUNTA DE GALICIA

UNIÓN EUROPEA

FONDO EUROPEO
DE DESARROLLO REGIONAL
"Una manera de hacer Europa"

gain

galicia

Annex I. About Triki

The tool that we have used for this analysis and that we have released is called **Triki**. It allows automated browsing, based on Selenium, on a set of websites for which a configuration has previously been defined in a yaml file that allows the relevant browsing flows to be carried out and the associated cookies to be extracted and high level statistics of its main characteristics.

It has an auxiliary script to load all the information collected in a SQLite database to facilitate its subsequent analysis.

By releasing them, we invite readers of this report to configure and check how their websites of interest manage cookies and whether or not they adhere to the regulations in force.

All information about its use is included in the tool's **README** within ElevenPaths' Github.

Annex II. Main Data of Our Analysis

Below, we present the main numbers in terms of number of cookies for each browsing flow of the Alexa Top100 Spain anonymised sites. The table presents the number of cookies for each flow in two big blocks without the blocking of third-party cookies activated and with the blocking active in the browser.

SITEID	NO THIRD-PARTY BLOCKING				THIRD-PARTY BLOCKING			
	BROWSE	ACCEPT	REJECT	TOTAL	BROWSE	ACCEPT	REJECT	TOTAL
Site001	4	10		14	4	8		12
Site002	5	9		14	4	5		9
Site003	5	10		15	4	8		12
Site004	8	8	8	24	6	6	6	18
Site005	4	12		16	3	11		14
Site006	4	46	18	68	3	10	10	23
Site007	46	74	50	170	17	27	22	66
Site008	4			4	3			3
Site009	1	2	2	5		1	2	3
Site010	9	14	12	35	8	11	11	30
Site011	30	99	33	162	36	29	24	89
Site012	15	15	15	45	6	6	6	18
Site013	3	20	8	31	2	16	7	25
Site014	40			40	23			23
Site015	26	28		54	23	25		48
Site016	27	130	29	186	19	24	21	64
Site017	16	16		32	15	15		30
Site018	14	15		29	11	14		25
Site019	58	107	46	211	29	34	33	96
Site020	66	83	52	201	37	41	40	118
Site021	10	12		22	10	10		20
Site022	8	11	9	28	7	10	8	25

SITEID	NO THIRD-PARTY BLOCKING				THIRD-PARTY BLOCKING			
Site023	14	88		102	9	9		18
Site024	8			8	7			7
Site025	6			6	5			5
Site026	13			13	10			10
Site027	19	60	25	104	15	27	15	57
Site028	6	8	8	22	5	7	7	19
Site029	27	27	23	77	6	8	7	21
Site030	36	43	39	118	20	22	22	64
Site031	7	38	8	53	6	11	7	24
Site032	6			6	5			5
Site033	21	21		42	18	17		35
Site034	12			12	9			9
Site035	22	92	23	137	17	26	18	61
Site036	10			10	9			9
Site037	4	5		9	3	4		7
Site038	13	14	14	41	7	8	8	23
Site039	7	8	8	23	4	5	5	14
Site040	6			6	5			5
Site041	18	132	22	172	14	23	15	52
Site042	17			17	12			12
Site043	12	32	12	56	11	22	13	46
Site044	16	68	20	104	13	25	17	55
Site045	6	16	7	29	3	8	4	15
Site046	7	8		15	6	7		13
Site047	6	7		13	5	6		11
Site048	23	22		45	19	19		38
Site049	4			4	1			1
Site050	10	11	16	37	8	8	13	29
Site051	5			5	4			4
Site052	27	183	29	239	22	23	24	69
Site053	10	11	11	32	9	10	10	29
Site054	53	100	119	272	15	18	13	46
Site055	20	20		40	13	13		26
Site056	14	20	16	50	17	17	15	49
Site057	23	32	20	75	16	25	11	52

SITEID	NO THIRD-PARTY BLOCKING				THIRD-PARTY BLOCKING			
Site058	7	8		15	6	7		13
Site059	25	152	39	216	10	19	18	47
Site060	28	65	30	123	13	18	15	46
Site061	28	35	31	94	24	30	28	82
Site062	2	4		6	1	3		4
Site063	15	20	16	51	10	15	8	33
Site064	7	8		15	6	7		13
Site065	5	23	12	40	4	15	11	30
Site066	50	51	52	153	31	32	34	97
Site067	17	59	19	95	16	35	18	69
Site068	29	38	33	100	6	12	10	28
Site069	41	136	43	220	7	9	8	24
Site070	10	11	11	32	4	5	5	14
Site071	21	67	22	110	9	12	13	34
Site072	4			4	3			3
Site073	6			6	4			4
Site074	16	18		34	15	17		32
Site075	1	5		6		4		4
Site076	14	134	17	165	8	12	11	31
Site077	13	66	21	100	9	12	10	31
Site078	8	8		16	7	7		14
Site079	5			5	4			4
Site080	10			10	9			9
Site081	11	15		26	9	13		22
Site082	52	83	21	156	10	15	14	39
Site083	2	8	3	13	1	7	2	10
Site084	8	22	11	41	6	12	9	27
Site085	51	80	37	168	21	24	24	69
Site086	20	49	24	93	18	30	22	70
Site087	7			7	3			3
Site088	25	151	27	203	20	21	22	63
Site089	6	8		14	5	7		12
Site090	36	44	38	118	33	38	39	110
Site091	16	28	18	62	6	10	8	24
Site092	4	30	6	40	3	15	4	22

SITEID	NO THIRD-PARTY BLOCKING				THIRD-PARTY BLOCKING			
Site093	70	83	54	207	38	41	41	120
Site094	78	78		156	17	17		34
Site095	10	13	10	33	9	12	8	29
Site096	15	29	16	60	12	12	13	37
Site097	19	55	17	91	10	12	12	34
Site098	9			9	6			6
Site099	4			4	3			3
Site100	8	47	12	67	4	31	12	47
Total	1.724	3.518	1.342	6.584	1.058	1.267	8.33	3.158

About ElevenPaths

ElevenPaths is Telefónica's cybersecurity company, part of the Telefónica Tech holding, which brings together the digital businesses with the greatest growth potential in the company.

In a world in which cyberthreats are inevitable, as intelligent managed security services suppliers, we focus on preventing, detecting, responding and diminishing the possible attacks faced by companies. We guarantee the cyberresilience of our customers through 24/7 support entirely managed from eleven i-SOCs around the world with global operational capacity.

We believe in challenging the current state of security, a characteristic that must always be present in technology. We are constantly rethinking the relationship between security and people with the aim of creating innovative products capable of transforming the concept of security. In this way, we manage to stay one step ahead of our attackers, whose presence is increasing in our digital lives.

We work to guarantee a safer digital environment through strategic alliances that allow us to improve the security of our clients. Besides constant collaborations with leading organisations and entities such as the European Commission, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, EuroPol, Incibe, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Industrial Cybersecurity Centre (CCI) y APWG.

elevenpaths.com | **@ElevenPaths** | **blog.elevenpaths**

ElevenPaths

Telefónica CYBER SECURITY COMPANY

This document is intended solely to support its reader in the use of the product or service described herein. The reader is committed and obliged to use the information contained herein for personal use and not for any other.

ElevenPaths shall not be liable for any loss or damage arising from the use of the information contained herein or for any errors or omissions in the document or for the misuse of the service or product. The use of the product or service described herein shall be governed by the terms and conditions accepted by the user of this document for its use.