COOKIE POLICY

We greatly value your choices

Cookies

To make this site work well, sometimes we install small data files called "cookies" on your device.

What are cookies?

A cookie is a small text file that websites save on your computer or mobile device while you visit them. Thanks to cookies, the site remembers your actions and preferences (eg login, language, font size and other display settings) so that you do not have to re-enter them when you return to the site or browse from page to page.

Types of cookies

The great variety of cookies in the web world makes it difficult to classify them. It is however possible to draw up a general list by separating them into different categories. The main attribute by which we can divide cookies is their life cycle, which allows us to distinguish them in:

- **Session cookies:** these cookies are not stored permanently on the user's device and are deleted when the browser is closed. Unlike other cookies, session cookies do not have an expiration date, and based on this the browser is able to identify them as such.
- **Persistent cookies:** instead of disappearing when the browser is closed, as is the case with session cookies, persistent cookies expire on a specific date or after a certain period of time. This means that, for the entire life of the cookie (which may be long or short depending on the expiration date decided by its creators), its information will be transmitted to the server each time the user visits the website, or whenever the user views a resource belonging to that site from another site (for example, an advertisement or an article). For this reason, persistent cookies can be used by advertisers to record information on a user's web browsing habits, anonymously, for an extended period of time. However, they are also used for "legitimate" reasons (such as keeping users registered in their account on the websites, in order to avoid, at each visit, the inclusion of credentials for access to the websites).

It is then possible to classify cookies based on their source, in:

- **First-party cookies:** normally, the domain attribute of a cookie will correspond to the domain that is displayed in the address bar of the web browser; these cookies are sent to the browser directly from the site you are visiting. This is called a first-party cookie. They can be both persistent and session; they are managed directly by the owner and / or responsible for the site and are used, for example, to ensure its technical functioning or keep track of preferences expressed regarding the use of the site.
- **Third-party cookies:** third-party cookies belong to domains other than those shown in the address bar. These types of cookies usually appear when web pages have content, such as banner ads, from external websites. This implies the possibility of monitoring the browsing history of the user, and is often used by advertisers, in an attempt to serve relevant and personalized ads for each user. For example, suppose a user visits www.example.org. This website contains an ad daad.foxytracking.com, which, once downloaded, sets a cookie that belongs to the advertising domain (ad.foxytracking.com). Therefore, the user visits another website, www.ooo.com, which also contains an ad from ad.foxytracking.com/, and which also establishes a cookie belonging to that domain (ad.foxytracking.com). In the end, both these cookies will be sent to the seller when they upload their advertisements or by visiting their website. The advertiser can then use these cookies to build a browsing history of users on all sites that have ads from this advertiser. Most modern web browsers contain privacy settings that are able to block third-party cookies.

Finally, it is possible to distinguish them from the use point of view (or finality) in:

- **Technical cookies:** they are used for navigation and to facilitate access and use of the site by the user. Technical cookies are essential without having to log in to all sessions. They are also in very sensitive operations such as home banking or credit card payments or other systems.
- **Statistical or "Analytic" cookies:** they are used to optimize the site, directly by the owner of the site, which can collect information in aggregate form on the number of users and how they visit the site. Under these conditions, the same rules apply to analytics cookies, in terms of information and consent, provided for technical cookies.
- **Cookies for storing preferences:** these cookies are useful to facilitate the correct use of the site by the user. They are used, for example, to keep track of the chosen language.

- **Advertising cookies:** these cookies are intended to provide advertising space. They can be installed by the site owner or by third parties. Some serve to recognize individual advertisements and know which ones have been selected and when. Other advertising cookies are used to hypothesize a "profile" of the user's navigation, in order to propose advertising messages in line with his behavior and interests in the network. This "profile" is anonymous and the information collected through these cookies does not allow us to trace the identity of the user. In this case, the cookie presides over one of the systems for piloting the so-called "behavioral advertising".
- **Social network cookies**: these are cookies that allow you to share the contents of the site you are visiting with other users. Cookies are typically used to activate the "Like" or "Follow" features of Social Networks such as Facebook and Twitter, just to name a few. These functions allow Social Networks to identify their users and collect information even while browsing other sites.

Other useful types of cookies:

- **Secure cookies:** a cookie with the Secure flag can only be transmitted over an encrypted connection (ie HTTPS). This decreases the probability of being exposed to the theft of cookies through eavesdropping. To achieve this, browsers that support this flag will only send cookies with the Secure flag when an HTTPS page is requested. In other words, the browser will not send a cookie with the Secure flag on an HTTP request, that is on an unencrypted connection.

- **HttpOnly cookies:** cookies with the HttpOnly flag can only be used if transmitted via HTTP (or HTTPS). They are not accessible through non-HTTP APIs like Java Script.
This restriction eliminates the threat of cookie theft through cross-site scripting (XSS), avoiding the threats of cross-site Tracking (XST) and cross-site request forgery (CSRF).

● **SameSite cookies:** Google Chrome 51 has introduced a new SameSite flag that allows the sending of cookies only for requests coming from the same source, thus managing to neutralize attacks such as CSRF and other types of attacks.
● **Super Cookie:** The "supercookie" is a cookie with an origin of a top-level domain (for example .com) or a public suffix (such as.co.uk). Ordinary cookies, on the contrary, originate in a specific domain, for example example.com. Supercookies can be a potential security problem and are therefore often blocked by web browsers. If unlocked by the client computer, an attacker, through a malicious website, could set up a supercookie, and potentially destroy or redirect requests from legitimate users to another website that shares the same top-level domain or public suffix of the website malevolent. For example, a supercookie with domain.com could maliciously influence an advanced request at example.com, even if the cookie did not originate from example.com. This can be used to make false accesses or modify user information. The Public Suffix List helps to reduce the risk that can be created through supercookies. This list is a cross-cutting initiative that aims to provide an accurate and up-to-date list of domain names. Older versions of browsers can not have an updated list, and will therefore be vulnerable to supercookies from certain domains.

● **Zombie cookies:** Zombie cookies are cookies that are recreated automatically after being deleted. This is achieved by storing the contents of the cookie in multiple locations, such as flash local storage, HTML5 storage, and through other storage mechanisms both by the client and by the server. When the absence of the cookie is detected, the cookie is recreated using the data stored in these locations.

How do we use cookies?

In some pages we use cookies, if you have authorized their use on our site, to remember:
• viewing preferences, e.g. contrast settings or font sizes.
• the language you prefer to browse our site.
• to give you the opportunity to save your login data.
• to protect yourself while making a purchase or payment on our site.
• to collect statistics in order to improve your browsing experience on our site.
• to protect your browsing on our site.

In addition, some videos inserted or that we insert in our pages use a cookie to process statistics, anonymously, on how you arrived on the page and which videos you saw.
It is not necessary to enable cookies for the site to work, but to improve navigation. You can delete or block cookies, but in this case some features of the site may not work properly.
The information regarding cookies is not used to identify users and navigation data are always under our control. These cookies are used exclusively for the purposes described here.

Which cookies* we use

Our site uses the following type of cookies:
• Session cookies.
• Persistent cookies - Technical cookies.
• First-party cookies.
• Cookie for storing preferences.
• Analitycs (statistical) cookies.
• SemSite Cookie.
• Secure Cookie.

Which cookies we DO NOT use

Our site does NOT use the following type of cookies:
• Third party cookies.
• Zombie Cookie.
• Super Cookie.
• Advertising cookies.
• Social network cookies.
• HttpOnly Cookie.

Duration of cookies

Some cookies (session cookies) remain active only until the browser is closed or when the logout command is executed.
Other cookies "survive" when the browser is closed and are also available in subsequent visits by the user. These cookies are called persistent and their duration is set by the server when they are created. In some cases a deadline is set, in other cases the duration is unlimited.

ENIGMA informs you that the information is stored exclusively for technical purposes.
However, browsing the pages of the enigmasolutions.it websites, it can take place the interaction with sites managed by third parties that can create or modify permanent and profiling cookies.

*The use of cookies on the site www.enigmasolutions.it may vary depending on the needs of development or updating of the web systems of ENIGMA Srls. If there is a variation of the cookies used, the user will be informed in advance through the integration and modification of this document, "COOKIE POLICY".

How to control cookies?

You can check and / or verify the use of cookies, to learn more go to the following section, Deactivate Cookies (Page 3). You can delete cookies already on your computer and set almost any browser to block its installation. If you choose this option, however, you will need to manually change some preferences each time you visit our site and it is possible that some services or certain features are not available.
For more information you can contact us on: info@enigmasolutions.it

To view how to disable cookies from your browser, see the cookie deactivation guide.

The procedure outlined below describes how to block the installation of new cookies and how to remove existing cookies.

The exact procedure, however, depends on the browser used.

Browser:
Internet Explorer 9.0+
Internet Explorer 8.0+
Internet Explorer 7.0+
Firefox 2.0+, 3.0+, 4.0+
Google Chrome
Safari

Many browsers automatically accept cookies. At any time, for Users who so wish, Cookies can be disabled or deleted from the browser. If cookies are deactivated, ENIGMA can not guarantee the correct functioning of the Site and to use all the services offered. These are the methods to be followed for deactivating cookies depending on the browser used for navigation:

Disabling cookies on your browser

Internet Explorer 9.0+

Block the installation of new cookies
- Select Tools on the menu bar
- Click Internet Options
- Click on the Privacy tab at the top
- Move the cursor to the "Block all cookies" button

Remove existing cookies
- Select Tools on the menu bar
- Click Options
- Click on the Privacy tab
- Click on "Cancel now"
- Select "Cookies"
- Click on "Delete personal data now"

Internet Explorer 8.0+

Block the installation of new cookies
- Select Tools on the menu bar
- Click Internet Options
- Click on the Privacy tab at the top
- Click on "Sites"
- A new window called "Managing privacy by site" should open
- Enter the site URL in the "Website Address" box and click Lock

Remove existing cookies
- Select Tools on the menu bar
- Click on 'Internet Options'
- Click on the Privacy tab at the top
- Click on "Sites"
- A new window called "Managing privacy by site" should open
- The "Managed Websites" box should include a list of all websites visited
- To remove all cookies, click on the "Remove all" button

Internet Explorer 7.0+

Block the installation of new cookies
- Select Tools on the menu bar
- Click Options
- Click on the Privacy tab at the top
- Click on the Advanced button
- Select "Ask confirmation" for both "Displayed website cookies" and "Third-party cookies" options

Remove existing cookies
- Select Tools on the menu bar
- Click Options
- Click on the General tab at the top
- In the "Browsing history" section, click on "Delete"
- Click on "Delete cookies"

Firefox 2.0+, 3.0+, 4.0+

Block the installation of new cookies

- Select Tools on the menu bar
- Click Options
- Click on the Privacy tab
- Uncheck the "Accept cookies from sites" box

Remove existing cookies

- Select Tools on the menu bar
- Click Options
- Click on the Privacy tab
- Click on "Cancel now"
- Select "Cookies"
- Click on "Delete personal data now"

Google Chrome

Block the installation of new cookies

- Click on the wrench icon at the top right of the browser
- Click on "Options"
- Click on "Under the Hood"
- Click on the "Content settings" button in the Privacy section
- Make sure that the option "Allow data saving locally" is select

Remove existing cookies

- Select "Prevent sites from setting data"
- Click on the wrench icon at the top right of the browser
- Click on "Options"
- Click on "Under the Hood"
- Click on the "Content settings" button in the Privacy section
- Click on the "Clear browsing data" button

Safari

Block the installation of new cookies and remove existing cookies

- Go to the Safari menu (icon at the top right of the browser) and select Preferences
- In the pop-up window that opens, select the Security icon (lock icon)
- Under "Accept cookies", select the "Never" button

©ENIGMA 2018