COOKIES PRIVACY POLICY

The website CLAIR DI BINDONI CHIARA VIA DERETTI 89/91 - 25013 CARPENEDOLO (BS) the data controller of your personal data, refers you to this Cookies Policy. As far as data processing is concerned, the data controller provides, among other things, the following information.
This policy on cookies ("Cookies Privacy Policy") should be read together with the Privacy Policy which may be consulted, in a separate document, under the Privacy section of the home page. This Cookies Privacy Policy is aimed at describing the different types of Cookies and technologies used in the website to describe their methods and terms of use.

This document contains the following information:
1. What is a cookie?
2. Types of cookies.
3. Third-party cookies.
4. Cookies Privacy and Safety.
5. Other threats from cookies.
6. Cookies in this site.

1. What is a cookie?
Cookies are small text files sent to the device (usually to the browser) from the sites visited by the user; they are stored on the computer under the relevant browser folder while the user is navigating a website and they are re-forwarded during later visits. The purpose is: to improve the navigation experience (the http protocol is stateless and is not able to “remember” the logged user who is reading the pages), to save the user’s preferences already inserted (username, password, etc), to track the user’s preferences in order to manage the presence of any possible focused marketing initiatives or provisions of services connected to the Controller’s activity such as newsletters, dem., etc.
Should any restrictions to their use be implemented, there will be definite effects on the status of the user during navigation. The block or removal of such cookies from the cache of the browser could result in an incomplete fruition of the services provided by the web app.

2. Types of cookies

Session cookies are created temporarily in the browser's subfolder while visiting a website. Once the user leaves the site, the session cookies are deleted.
They are usually used to identify the users when accessing a website, to remember the user and his/her preferences in moving from page to page, to provide him/her with specific information previously obtained. The most common example of this functionality is the shopping cart feature of any e-commerce site. For example, when you visit one page of a catalogue and select some items, the session cookie remembers your selection so your shopping cart will have the items you selected when you are ready to check out. Without session cookies, if you click CHECKOUT, the new page does not recognize your past activities on prior pages and your shopping cart would always be empty.

Persistent cookies remain activated even after you have closed the browser and they help websites remember your information and settings when you visit them in the future. This results in faster and more convenient access as there is no need to log in again.
Besides authentication, other website features made possible by persistent cookies include: language selection, theme selection, menu preferences, internal site bookmarks or favourites, among many others.
During the visit, you can select your preferences and these preferences are remembered through the use of the persistent cookie the next time you visit the site.

3. Third-party cookies

There are different types of cookies; some of them are called third-party cookies.

They are used, for example, by the first site that the user has visited and they contain advertisements from another server or a third-party site.
The browser assembles the information fed from differing sources so all items appear on the same page thus creating a cookie in the relative browser's folder.
All these cookies can be removed directly from the browser setting or it is possible to prevent them from being created. In this case some services provided by the site might not operate as usual and it might not be possible to access the site or the user's preferences could be lost if there is no associated cookie; the information could be displayed in a wrong local format or not be available.

Web Beacons : also called "tracking pixels", "gifs 1x1", "pixel gifs", "pixel tags" or "action tags" are graphic images usually no larger than 1 pixel x 1 pixel that are used to collect anonymous information concerning the behaviour of the user visiting the website and to offer personalised contents. They also allow for the identification of the type of browser and the words inserted by the users in the search engines to reach the website.
Web Beacons present in e-mails allow the user to know if he has received opened or clicked on the links provided by the e-mail received.

Flash Cookies or Local shared objects (LSOs): the websites may use Flash contents displayed in the pages to record some information on the device.
Similar to HTTP cookies, Local Shared Objects may be used by the websites to collect information or to track the user's internet activity when navigating between websites. Online banks and advertisers can use Local Shared Objects for monitoring purposes.

Functionality cookies are used to provide enhanced services and to remember the settings in order to improve the surfing experience such as providing the user with the last site accessed. They are never used for any purposes other than those described and sometimes they are "strictly necessary" for the functionality/services implemented on the website.

Google Analytics is a service offered by Google which generates detailed statistical surveys concerning the traffic of a website and the traffic source. It is the most used statistical service. Google Analytics can monitor visitors coming from links external to the site such as search engines and social networks, direct visits and reference sites. It also displays advertisements, pay-per-click, e-mail marketing and links inside PDF files.
You can access informative notice at the following address:
http://www.google.it/analytics/learn/privacy.html

4. Cookies privacy and safety

Cookies are not viruses, they are only text files which are not interpreted by the browser or recorded. Consequently they cannot be duplicated and disseminated in other networks to be replicated again. Since they cannot carry out these functions, they are not by definition deemed to be viruses.
On the other hand, Cookies can be used for harmful purposes.
Since information concerning preferences, the history of the users and the specific navigation between different websites are recorded, cookies can be used as a form of spyware.
Many anti-spyware products are aware of this issue and they commonly point out Cookies as possible threats.

As regards Flash Cookies, Adobe does not directly supply a tool to personalise the setting of Flash Player connected to its management. Instead, to access the various setting offered, it is necessary to access any web page including the creative contents, right click on the mouse, choose Global Storage Settings and then click on the "General setting Panel" link of the privacy page. Alternatively, it is possible to visit the page directly:

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html
It is worth noting that by eliminating Flash cookies or deactivating the memory completely some web sites will not operate in the expected way. Flash cookies can be used, for example, to force a new creation of traditional HTTP cookie containing information it held previously.

5. Other threats from cookies

As cookies are transmitted between browsers and websites, a malicious or unauthorised user could intercept the transmission of data and information relative to it. Even if it is relatively rare, this could happen if the browser is connected to the website using a non-protected WI-FI network, for example. Other attacks due to cookies involve the setting of the server. If a website does not request the browser to use only encrypted connections (i.e. https), a malicious person could take advantage of this vulnerability to trick the visitors by forwarding personal information via insecure channels and could then direct such personal data for unauthorised treatment.

6. Cookies in this site

No personal data of the User is stored by the website. No cookies are used for transmission of information of a personal nature, no persistent cookies of any type are used, that is, systems for tracking the User. Use of the so-called session cookies – which are not stored permanently on the user's computer and disappear upon closing the browser – is exclusively limited to the transmission of session ID's – consisting of server-generated casual numbers – as necessary to allow secure, effective navigation.
The session cookies used by this website make it unnecessary to implement other computer techniques that are potentially detrimental to the confidentiality of user navigation, whilst they do not allow acquiring the user's personal identification data.

Third party cookies may be present on our website; we hereby provide you with the relevant links:
Google Analytics (http://www.google.it/analytics/learn/privacy.html),
Google Maps / You tube / Google+ (http://www.google.com/intl/it/policies/privacy/)
Twitter (https://support.twitter.com/articles/20170519-uso-dei-cookie-e-di-altre-tecnologie-simili-daparte-di-twitter)
Facebook (https://www.facebook.com/help/cookies)
Linkedin (https://www.linkedin.com/legal/cookie_policy)
Addthis (http://www.addthis.com/privacy/privacy-policy#publisher-visitors)

It is possible to disallow general consent to the use of cookies by selecting the appropriate setting of your browser: navigation without tracking of history will however be available in all its functionality. Here below the links on how to disable cookies on the most used browsers are listed:
Microsoft Edge: https://privacy.microsoft.com/it-it/windows-10-microsoft-edge-and-privacy
Internet Explorer: http://windows.microsoft.com/it-it/windows7/block-enable-or-allow-cookies
Google Chrome: https://support.google.com/chrome/answer/95647?hl=it-IT&p=cpn_cookies
Mozilla Firefox: https://support.mozilla.org/it/kb/Attivare%20e%20disattivare%20i%20cookie
Apple Safari: https://www.apple.com/legal/privacy/it/cookies/

The user who is visiting our website fully accepts the abovementioned notice.