

## Sessions

- HTTP is stateless. Each request for a Web page or URL results in the requested pages being served, but without the Web (HTTP) server remembering the request later. In other words, there is no recorded continuity. Each communication is discrete and unrelated to those that precede or follow
- Server side technologies can implement state or server side sessions using one or more of the following methods:
  - **HTTP cookies**
    - main use:
      - identify users
      - remember users' custom preferences
      - help users complete tasks without having to re-enter information when browsing from one page to another or when visiting the site later
    - cookies types classified by its lifespan:
      - *session cookies*
        - A user's session for a website exists in temporary memory only while the user is reading and navigating the website. Web browsers normally delete session cookies when the user closes the browser
      - *persistent cookie*
        - remains on the user's computer/device for a pre-defined period of time
    - cookies types classified by its domain:
      - *first-party cookies*
        - set by the web server of the visited page and share the same domain
      - *third-party cookies*
        - stored by a different domain to the visited page's domain. This can happen when the webpage references a file, such as JavaScript, located outside its domain
    - EU legislation
      - *EUROPA websites must follow the Commission's guidelines on privacy and data protection and inform users that cookies are not being used to gather information unnecessarily*
      - *you must ask users if they agree to most cookies and similar technologies (e.g. web beacons, Flash cookies, etc.) before the site starts to use them*

- *Cookies clearly exempt from consent*
  - user-input cookies (session-id) such as first-party cookies to keep track of the user's input when filling online forms, shopping carts, etc., for the duration of a session or persistent cookies limited to a few hours in some cases
  - authentication cookies, to identify the user once he has logged in, for the duration of a session
  - user-centric security cookies, used to detect authentication abuses, for a limited persistent duration
  - multimedia content player cookies, used to store technical data to playback video or audio content, for the duration of a session
  - load-balancing cookies, for the duration of session
  - user-interface customisation cookies such as language or font preferences, for the duration of a session (or slightly longer)
  - third-party social plug-in content-sharing cookies, for logged-in members of a social network
- *Evaluate for each cookie if informed consent is required or not*
  - first-party session cookies DO NOT require informed consent.
  - first-party persistent cookies DO require informed consent. Use only when strictly necessary. The expiry period must not exceed one year.
  - all third-party session and persistent cookies require informed consent. These cookies should not be used on EUROPA sites, as the data collected may be transferred beyond the EU's legal jurisdiction
- *Before storing cookies, gain consent from the users (if required) by implementing the [Cookie Consent Kit](#) in all the pages of any website using cookies that require informed consent*
- *Inform users about the use of cookies in plain, jargon-free language in a dedicated "cookie notice" page linked from the service toolbar of the [standard templates](#). This page should explain:*
  - why cookies are being used, (to remember users' actions, identify users, collect traffic information, etc.)
  - if the cookies are essential for the website or a given functionality to work or if they aim to enhance the performance of the website
  - the types of cookies used (e.g. session or permanent, first or third-party)

- who controls/accesses the cookie-related information (website or third-party)
  - that the cookie will not be used for any purpose other than the one stated
  - how users can withdraw consent.
- A [standard template to create your own cookie notice page](#)
- Query string parameters, for example:  
/index.php?session\_id=some\_unique\_session\_code
- hidden variables within web forms