PRIVACY AND PERSONAL DATA PROCESSING CHARTER

Our principles, our ethics **2**
Some definitions **3**
Who is responsible for your data? **3**
What do we do with your information? **3**
What information do we process? **4**
Who has access to your information? **5**
How long before your information is deleted? **5**
What are your rights? **5**
How can I access my information? **5**
How can I correct and update my information? **6**
How can I delete my information? **6**
iNNERSHiP and advertising **7**
Manage your cookies **7**

Respecting your privacy and protecting your personal data is a top and ongoing priority for iNNERSHiP, which follows a “Privacy by Design” approach. This means that your personal data is protected by default, both in the design of our systems and in iNNERSHiP’s practices. All

processing is done transparently, respecting your rights as recognized by applicable laws and regulations, as well as by this Charter. Your privacy is protected throughout the entire process, from the design of the application to the deletion of your data.

iNNERSHiP provides a high level of protection in line with European personal data protection standards to all clients and users, regardless of their country of origin and, subject to legal and regulatory obligations, no matter where they access the services from. The processing of your personal data has been declared when required, for example to the Commission Nationale de l'Informatique et des Libertés (CNIL – www.cnil.fr) under number 2006807.

Our principles, our ethics

Our approach to privacy and personal data protection is based on the following principles:

- **Transparency and fairness**: you know what information is collected, by whom, how, and for what purposes. You can also request more details about the processing at any time by contacting our team.
- **Consent**: data is processed only with your explicit, free, and informed consent.
- **Your interests always come first**: we implement strict and implicit privacy protection measures for clients and users, as well as user-friendly design and experience, especially regarding information.
- **Accountability**: the activity of anyone accessing your data is recorded, and they may be required to justify their access.
- **Proportionality and legitimacy** : the personal data processing we carry out aims to minimize data. We only process information necessary to achieve specific, explicit, and legitimate purposes. The retention period for your data is also limited.
- **Anonymization**: as soon as it is no longer necessary to keep information in an identifiable form, it is deleted or anonymized.
- **Relevance and accuracy**: procedures for updating and correcting information are in place and always available to you.
- **Security and confidentiality**: we take all necessary precautions, considering the nature of the data and the risks involved in processing, to keep your data secure and, in particular, to prevent it from being altered, damaged, or accessed by unauthorized third parties.

Some definitions

- **Personal data**: this is data that identifies you directly or indirectly. Hereafter referred to as "Personal Data" or "Data".
- **Sensitive data**: this is data that directly or indirectly reveals ethnic origins, political, philosophical or religious opinions, union membership, or relates to health or sexual life. We never process sensitive data.

- **Personal data processing**: any operation carried out by any means involving Personal Data.
- **Data controller**: this is the person who decides the purpose and means of processing. Hereafter referred to as “the Controller”.

Who is responsible for your data?

The Controller is iNNERSHiP SAS, with its head office at Résidence Château Levat - 188 rue Alfred Cortot, 34000 MONTPELLIER, registered with the Montpellier Trade and Companies Register under number 811 488 113.

Its representative is: Thomas d’Hauteville, President of iNNERSHiP.

Please note that personal data processing is considered a company asset and may be transferred in the event of a sale. In such a case, unless you expressly consent otherwise, you will continue to benefit from this charter.

What do we do with your information?

Professional fulfillment is a personal and intimate matter, unique to each individual. Every user is free to address personal topics and move forward in Version 2.6 4 by answering the questions they choose. The Personal Data collected in this way allows everyone to progress in their personal reflection and benefit from the highest quality services. Processing is used in particular to help you design and achieve your professional projects and dreams, identify your preferences, strengths, and possible limitations, and thus develop your potential.

We guarantee the strictest confidentiality for your data, which is anonymized as soon as possible.

The processing carried out may also be used in the context of teaching, career mobility, or coaching activities.

We also process personal data to improve our services. For this purpose, we carry out statistics, and may use segmentation to offer you services best suited to your needs. If you have previously consented, we may occasionally use part of our newsletter to inform you about updates to our various services. We may also offer you promotional deals and occasionally send you commercial offers. However, if you no longer wish to receive these offers, you can opt out at any time and we will immediately stop sending them to you.

What information do we process?

The information we process includes: email and username (pseudonym), country of residence, preferred language. In the context of a company, university, school, or institution, we also process the name of the company, university, school, or institution involved, possibly with the department, program, or section that allows us to provide you with the service chosen by the client offering you this service.

We collect the information you provide when using our services, for example when creating your account and during your journey. You are always free to choose what information you wish to share. Please note that this information is processed by iNNERSHiP to provide you with the best possible service, and we guarantee its strict confidentiality. In particular, your employer does not have access to it.

Other information about you may be generated directly by your use of electronic communication networks. For example, your “internet protocol” address, the date and time of your connections to the iNNERSHiP application, the type of browser used, the operating system of the device you use to connect, etc. This information allows us to track your journey in the application so we can continually improve the quality of the service we provide and better adapt to your device. This information is also useful for prevention and diagnostics. We also use cookies, which we will explain in more detail and tell you how to delete later in this charter.

If the device you use to connect to the application allows it, we may use so-called “geolocation” information. Please remember that you can disable your device’s location function at any time and thus refuse us access to this data. In this case, we may also process the device’s unique identifier (IMEI/MEID, CDN, ICCID, etc.).

Who has access to your information?

The data entered by each individual as part of their journey in the application belongs to them. The only people who may have access to your information are those you have personally chosen to invite to your project to support you. For example, when you invite a companion on iNNERSHiP, they will receive an email containing the email address you used to sign up and the pseudonym you use on iNNERSHiP.

Under no circumstances can the company, university, school, or institution providing you with this service access this individual data. In particular, neither your supervisor nor authorized personnel responsible for managing staff or students can access your information related to your journey.

How long before your information is deleted?

Personal data is not kept by the managing services beyond the period of employment, school program, or contractual relationship with your coach, except where specific legal or regulatory provisions require a particular retention period or deletion of certain data. For example, data needed to prove a right or contract may be archived in accordance with applicable laws and any evidentiary needs. Subject to the above, information is deleted one year after the end of the contract.

Personal data relating to commercial prospects (companies or universities) is only kept for as long as it is needed for prospecting activities.

What are your rights?

By entering your data, you acknowledge that you have read this privacy and data protection charter and you fully consent to its application.

How can I access my information?

As long as you can prove your identity, you have the right to access information about yourself. You can, for example, obtain confirmation that we are processing information about you, and request additional information regarding:

- regarding the purpose of processing;
- regarding the purposes of processing, the categories of personal data processed, and the recipients or categories of recipients to whom the data is disclosed;
- if applicable, information about any planned transfers of personal data to a country outside the European Community;

To access your information, log in to your account using your username and password, then click on the “Profile” menu and select “Settings.”

How do I correct and update my information?

To edit and update your information (such as changing your email address, username, notification frequency, etc.), log in to your account using your username and password, then click on the “Profile” menu and select “Settings.”

How do I delete my information?

If your data is used for marketing purposes, you also have the right to object, which allows you to request the deletion of your information, subject to legal retention requirements and limitation periods.

You can exercise your rights and ask any questions about the protection of your privacy and personal data by writing to iNNERSHiP SAS at the following address: Résidence Château Levat - 188 rue Alfred Cortot, 34000 MONTPELLIER. Be sure to include a copy of a piece of government-issued identification with your letter.

This identity verification is intended to prevent any communication or destruction of data at the request of a third party attempting to impersonate the person concerned by the personal data processing.

iNNERSHiP does not transfer your data to countries outside the European Union, the European Economic Area, or to countries not recognized by a European Commission decision as providing adequate protection.

We guarantee the confidentiality, security, and integrity of your information.

We take all necessary precautions to protect the security of your data, especially to prevent it from being altered, damaged, or accessed by unauthorized third parties.

Your consent is key to controlling your data.

Based on the information provided in this Policy, you acknowledge that you have given your express, free, and informed consent to the processing of personal data described herein. This Policy is part of the general terms and conditions governing our services. By accepting our general terms, you expressly accept the provisions of this Policy. Please note that this Policy is accessible from our mobile app, and installing and using the iNNERSHiP mobile app means you consent without reservation to the terms of this Policy.

iNNERSHiP and advertising

Although iNNERSHiP does not currently display ads in its app, it reserves the right, unless you object, to use your data to offer you the most relevant and best-suited ads that provide real added value for you. To do this, we may rely on your use of the iNNERSHiP app. We do not share your information with advertisers or third parties.

Manage your cookies (connection tokens)

When you browse our website http://www.innership.com, your web browser may create cookies (connection tokens). These are text files (.txt) that store certain information, such as your display preferences or your device (computer, smartphone, tablet, etc.). The goal is to make your browsing experience on http://www.innership.com easier and better.

Third-party sites may also place “cookies” when displaying ads. Cookies are a common tool on the internet, and we are only responsible for cookies identified as coming from “http://www.innership.com.”

We do our best to ensure that these third-party sites strictly respect your privacy rights as well as applicable laws and regulations.

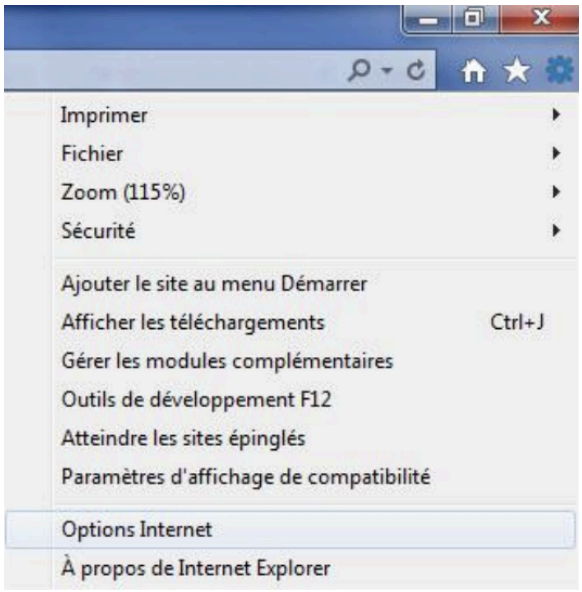
You can view and delete all cookies stored on your device at any time.

You can also set your web browser to notify you whenever a “cookie” is created, and set up automatic rules to define a specific cookie policy.

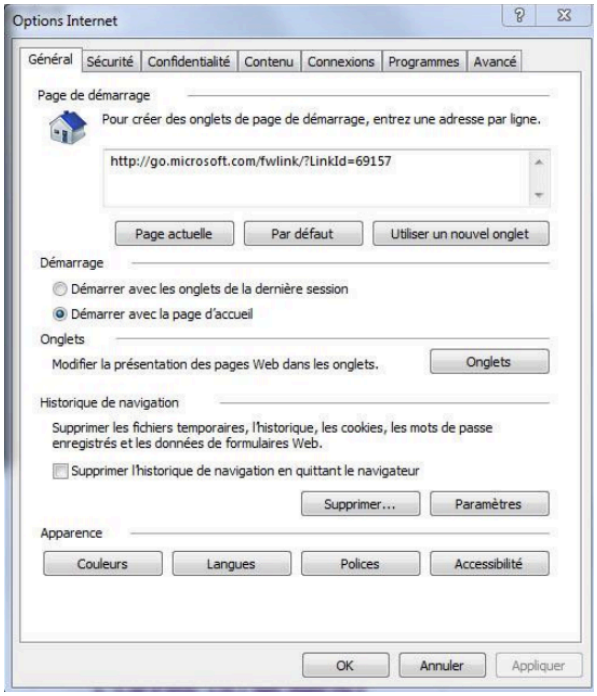
The following cookie management and deletion tutorials are current as of 2026-09-24, but they may change as software publishers update their products.

Internet Explorer

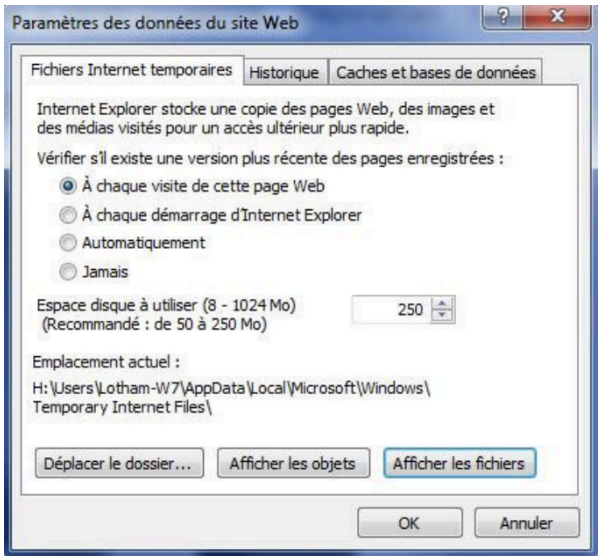
To manage your cookies with Internet Explorer, choose the “Tools” menu, then “Internet Options”:

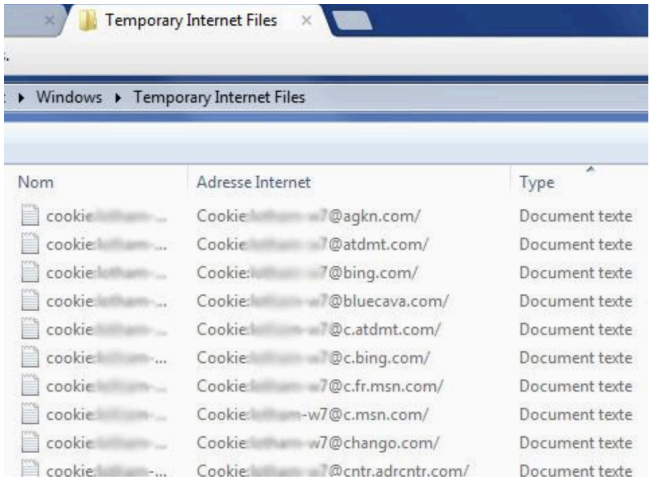


In the “Internet Options” window, under “Browsing history,” click on “Settings”:



Finally, click on “View files”:





To block third-party cookies:
Third-party cookies are usually not necessary to enjoy resources available on the Internet. If you want to limit your digital footprint, it is recommended to refuse them by default.

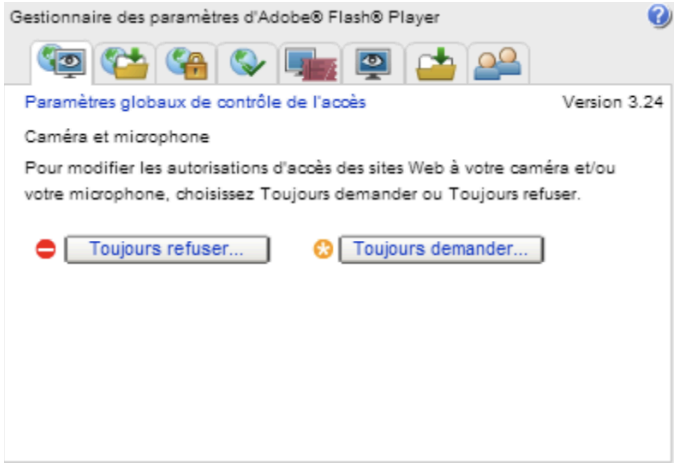
Menu > Internet Options > "Privacy" tab and click on the ***Advanced*** button to open the ***Advanced Privacy Settings*** window.

Then check the box "***Override automatic cookie handling***," then select "***Block***" in the "***Third-party Cookies***" column.

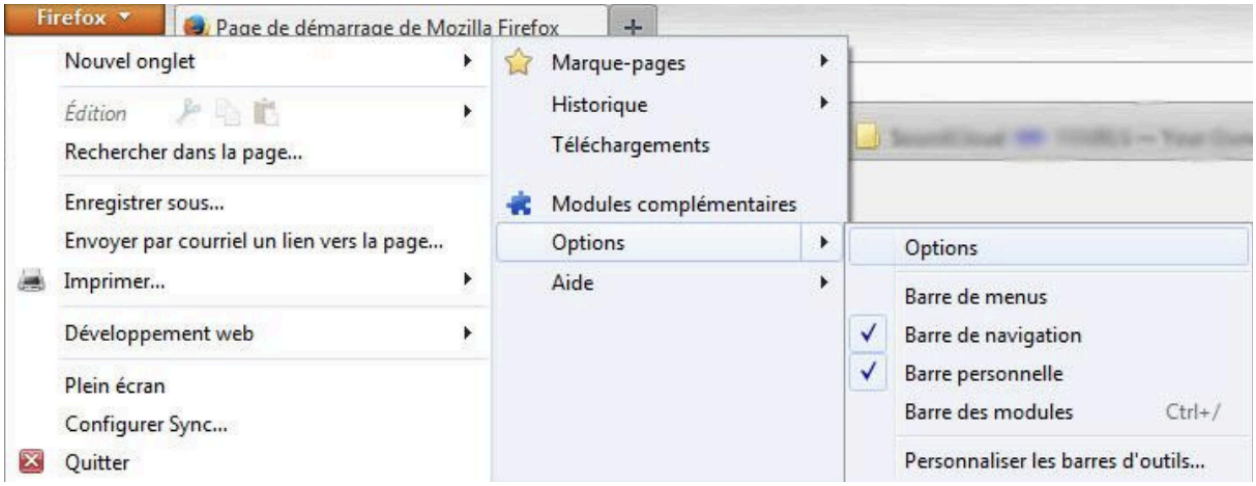
Limit tracking in Adobe Flash:
The Flash software component is set by default to allow the storage of information that can track users.

It is recommended to change these settings by accessing the online settings manager.

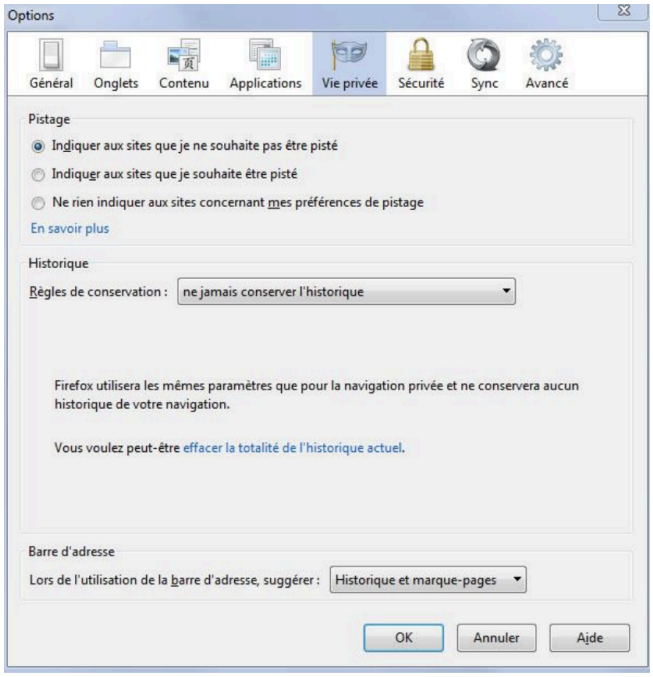
You need to set the privacy settings for each of the 8 tabs.



Firefox
In the "Firefox" menu at the top left of the window, choose the "Options" menu:



In the “Privacy” tab, click on “Clear All History”



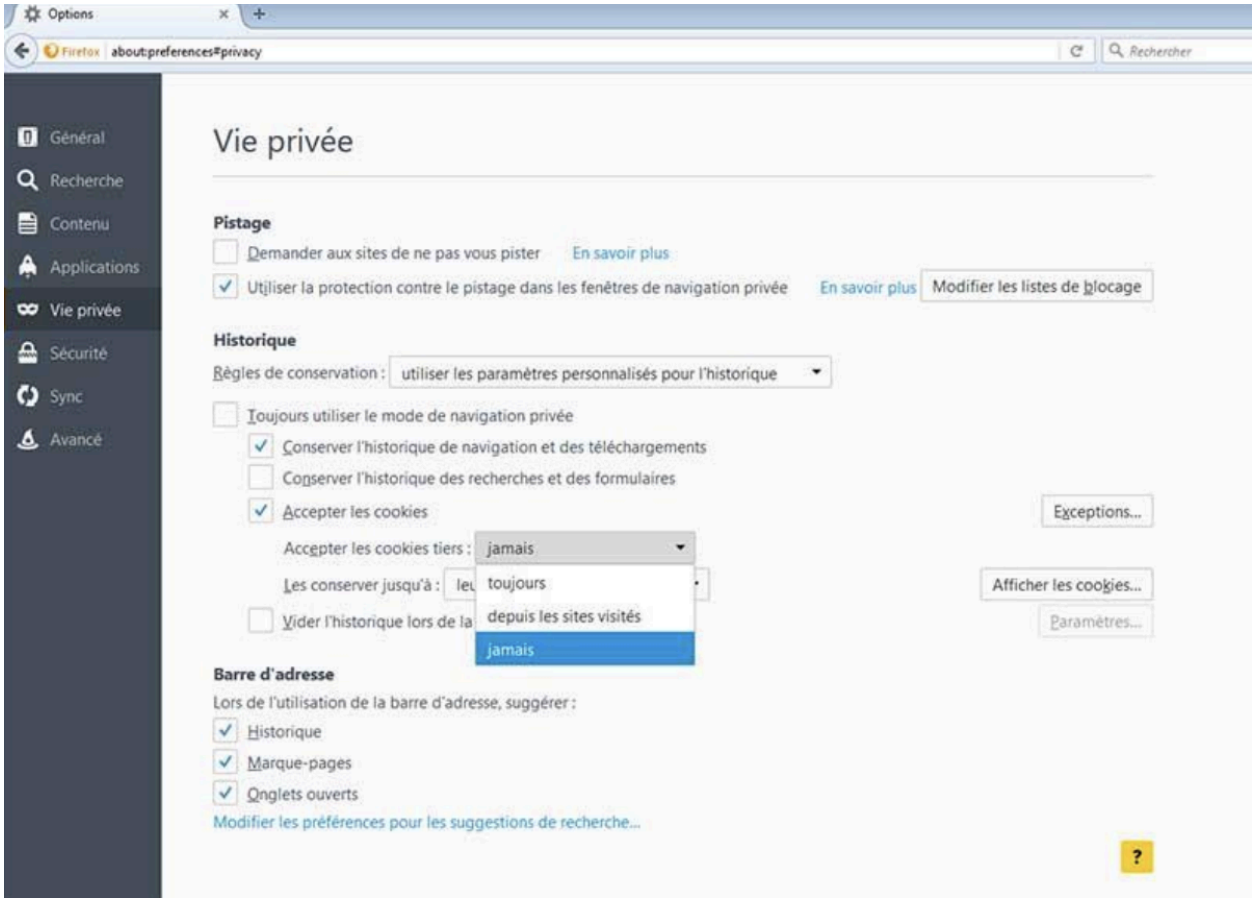
You can then choose which information to delete.

Block third-party cookies

Third-party cookies are usually not necessary to enjoy resources available on the Internet. To limit your digital footprint, it is recommended to refuse them by default.

In the Firefox browser: **Menu > Options > “Privacy” tab Set the “History” menu** to “**Use custom settings for history**.”

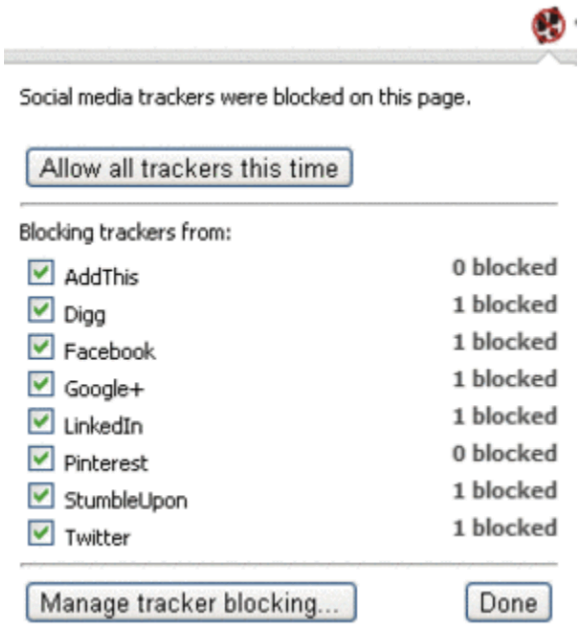
Finally, uncheck the box “**Accept third-party cookies**.”



Prevent tracker installation:
There are many Chrome extensions that can block different trackers.
Some examples:

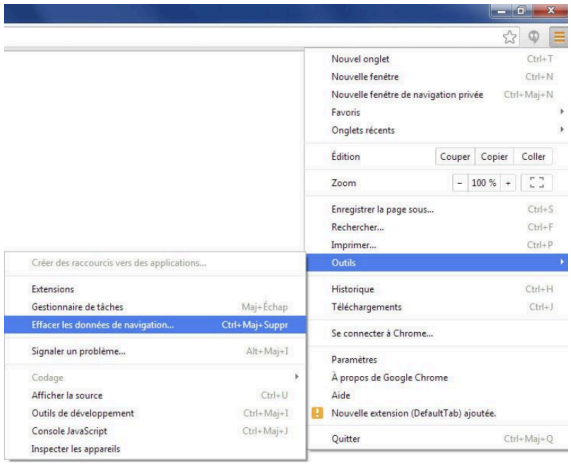
- DoNotTrackMe: A simple extension that blocks trackers.
- Disconnect: A very comprehensive extension that blocks trackers and offers advanced features. We highly recommend it.
- Ghostery: This excellent extension blocks trackers.
- Adblock: AdBlock goes beyond privacy protection and systematically blocks ads, including non-personalized ones, before they appear in your browser. However, these ads help fund websites, especially those offering free services to users. Therefore, this solution is only recommended as a last resort.

Share on social networks… or not:
When you visit sites with social media buttons, those networks are informed of your visit. It is therefore recommended to block this tracking unless you want to share the site you are visiting. This blocking of social media buttons like Facebook, Twitter, etc., can be achieved using a free and open-source extension: Share me not

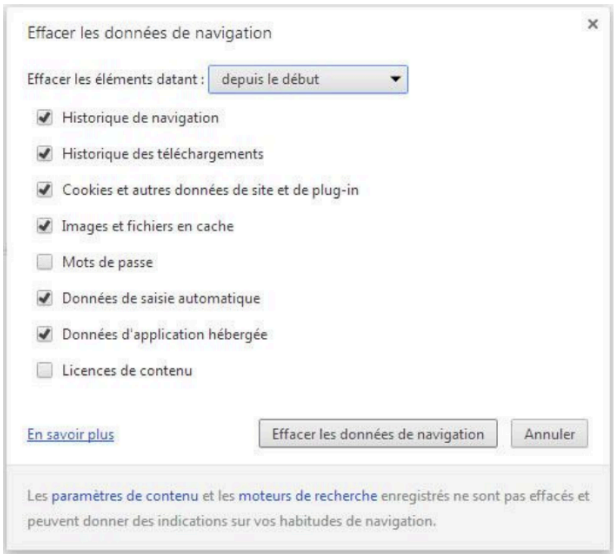


Google Chrome

Go to the menu at the top right of the browser window, click on “Tools,” then on “Clear browsing data.”

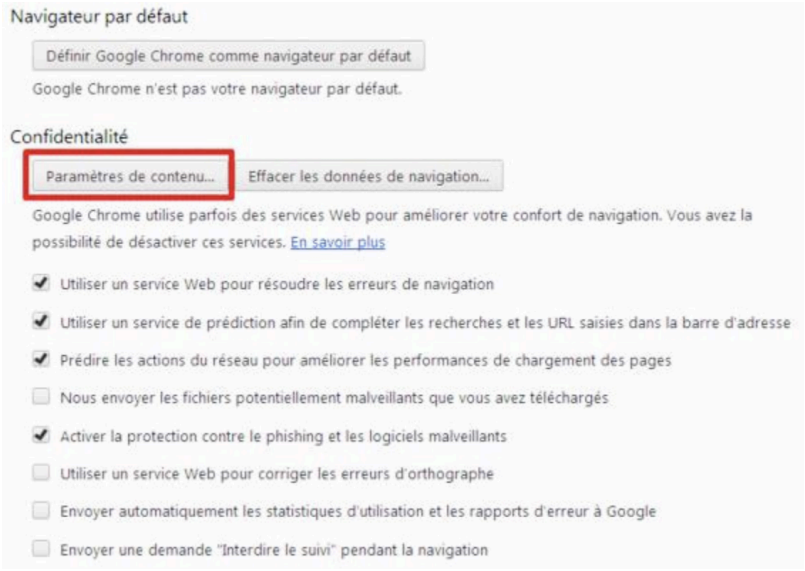


You can then delete cookies (also known as "témoins de connexion"):



Block third-party cookies:
Menu > Settings > Show advanced settings (at the bottom of the page).

Then click on the Content Settings button, check the box Block third-party cookies and site data, and finally click OK to confirm your choice.



Prevent tracker installation:
There are many Chrome extensions that can block different trackers.
Some examples:

- DoNotTrackMe: A simple extension that blocks trackers.
- Disconnect: A very comprehensive extension that blocks trackers and offers advanced features. We highly recommend it.
- Ghostery: This excellent extension blocks trackers.

- Adblock: AdBlock goes beyond privacy protection and systematically blocks ads, including non-personalized ones, before they appear in your browser. However, these ads help fund websites, especially those offering free services to users. Therefore, this solution is only recommended as a last resort.

Share on social networks… or not:
When you visit sites with social media buttons, those networks are informed of your visit. It is therefore recommended to block this tracking unless you want to share the site you are visiting. This blocking of social media buttons like Facebook, Twitter, etc., can be achieved using a free and open-source extension: Share me not



Safari
In your browser, choose the Edit menu → Preferences → Security → Click on Show Cookies.

For other browsers and mobile devices:
If you want to restrict the use of cookies for another browser or on a mobile device, you can visit the official website of the browser or device manufacturer or consult the documentation provided, then follow the instructions.