PRIVACY POLICY

Data collected on the basis of consent

Upon your request and explicit consent, we collect the following data for the purpose of providing services to you. Your data is not used for any other purposes nor will it be shared with third parties. It shall be removed upon your withdrawal of consent or your request to terminate theses services.

Comments

Name, email address, content of the comment: this data is collected when you leave a comment and displayed on the Website.

If you leave a comment on the Website, your name and email address will also be saved in the cookies. These are for your convenience so that you do not have to fill in your details again when you leave a future comment. These cookies will be saved on your computer until you delete them.

IP and browser user agent string: this data is collected when you leave a comment.

Retention period: the aforementioned data is retained indefinitely so we can recognize and approve any follow-up comments automatically instead of holding them in a moderation queue.

Data collected on the basis of legitimate interest

Based on our **legitimate interests**, we collect the following data for the purpose of running this website. Your data is not used for any other purposes or shared with third parties. It shall be removed upon your request.

Statistics

The website uses a minimal build of Google Analytics, a service which transmits website traffic data to Google servers in the United States and allows us to notice trends to improve the user experience on our website. This minimal build processes personal data such as: the unique User ID set by Google Analytics; date and time; the title of the page being viewed; the URL of the page being viewed; the URL of the page that was viewed prior to the current page; screen resolution, the time in local time zone; the files that were clicked on and downloaded; the links clicked on to an outside domain; type of device; and the country, the region, and the city.

You may opt out of this tracking at any time by activating the “Do Not Track”

setting in your browser.

Embedded content from other websites

Articles on the Website may include embedded content (e.g. videos, charts, etc.). Embedded content from other websites behaves in the exact same way as if the visitor had visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracing your interaction with the embedded content if you have an account and are logged in to that website.

Your rights pertaining to your data

If you have left comments on the Website, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we rectify or erase any personal data we hold about you. Please send your request to gdpr@themodern.press

- The right to withdraw consent
- The right of Access
- The right to deletion
- The right to rectification
- The right to data portability
- The right to object
- Notification of data breaches
- The right to lodge a complaint with a supervisory authority

RIGHT TO DELETION REQUEST FORM

You are entitled to request us to delete any personal data we hold about you under EU General Data Protection Regulation (GDPR).

We will do our best to respond promptly and in any event within one month of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request, whichever happens to be later.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting that we erase and responding to your request. You are not obliged to complete this form to make a request but doing so will make it easier for us to process your request quickly.

SECTION 1: Details of the person requesting information

Full name:

Address:

Contact telephone number:

Email address:

SECTION 2: Are you the data subject?

Please tick the appropriate box and read the instructions which follow it.

- YES: I am the data subject. I enclose proof of my identity (see below) (Please go to Section 4)

- NO: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below). (Please go to Section 3)

To ensure that we are deleting the data of the right person we request for you to

provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one or both of the following:

1) Proof of Identity

A copy of a Passport; a copy of your driver's license (it has to have a photograph); a copy of a national identity card; or a copy of a birth certificate.

2) Proof of Address

A copy of an utility bill; a copy of a current bank statement; a copy of a current credit card statement; or a copy of a current driver's license.

If we are not satisfied with your identity, we reserve the right to refuse to grant your request.

SECTION 3: Details of the data subject (<u>if different from section 1</u>)

Full name:

Address:

Contact telephone number:

Email address:

SECTION 4: Reason for request to delete

Given the sensitive nature of deleting personal data, GDPR Article 17(1) requires certain conditions to be met before a request may be considered. Please supply us with the reason why you wish your data to be deleted and please attach any justifying documents to this.

Please tick the appropriate box:

- You feel your personal data is no longer necessary for the purposes for which we originally collected it.

- You no longer consent to our processing of your personal data.

- You object to our processing of your personal data as is your right under Article 21 of the GDPR.

- You feel your personal data has been unlawfully processed.

- You feel we are subject to a legal obligation of the EU or Member State that requires the erasure of your personal data.

- You are a child, you represent a child, or you were a child at the time of the data processing and you feel your personal data was used to offer you information society services.

SECTION 5: What information do you wish to delete?

Please describe the information you wish to erase. Please provide any relevant details you think will help us to identify the information. Providing the URL for each link you wish to be removed would be helpful.

Also, please explain, if it is not abundantly clear, why the linked page is about you or the person you are representing on this form.

Please note that. Under certain circumstances, where deletion would adversely affect the freedom of expression; contradict a legal obligation; act against the public interest in the area of public health; act against the public interest in the area of scientific or historical research; or prohibit the establishment of a legal defense, or exercise of other legal claims, we may not be able to delete the information you requested in accordance with article 17(3) of the GDPR. In such cases you will be informed promptly and given full reasons for that decision.

While in most cases we would be happy to delete the personal data you requested, we nevertheless reserve the right, in accordance with Article 12(5) of the GDPR, to charge a fee or refuse the request if it is considered to be “manifestly unfounded or excessive.” However, we will undertake every effort to provide you with the deletion of your personal data if suitable.

SECTION 6: Declaration

Please note that any attempt to mislead may result in prosecution and/or judicial

proceeding.

I confirm that I have read and understood the terms of this subject access form and I certify that the information given in this application to theModern.Press is true and correct. I understand that it is necessary for theModern.Press to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to confirm the correct personal data.

Date:

……..

Signed:

……

Documents which must accompany this application:

- Evidence of your identity (see section 2)
- Evidence of the data subject's identity (if different from above)
- Authorization from the data subject to act on their behalf (if applicable)
- Justification for data deletion (see section 4)

PRIVACY STATEMENT FOR REGISTERED USERS

1. What is the Identity Management Service?

The Company's Identity Management Service (IMS) provides a common way for users to register, or to be registered for access to a number of different Company information systems, or services (referred to hereafter as *sites*).

This privacy statement would concern you if you use the Company authentication service (Login) when logging into the sites, as it means that you have been registered in IMS.

Users include the Company's own staff; staff (or employees) of other organizations; and members of the public.

Registration may occur:

- At the initiative of a user, or of the organization that the user belongs to or represents
- By means of an automatic transfer of information from the user's organization to the Commission
- By means of direct entry of the relevant information by the user

IMS includes facilities for authenticating registered users and controlling their access to Company sites.

In each case, the personal data that is recorded is governed by Regulation (EU) 2018/1725.

IMS falls under the responsibility of the Executive Chairman, Ö. Emre Ekşi. Further responsibility lies with each individual processor of the information.

Individual Company sites that rely on IMS for commonly required personal data may nevertheless collect additional personal data themselves. This is covered by the sites' own privacy statements.

2. What information do we collect, for what purpose and through which technical means?

In general, registration is required:

- if access to a site is restricted to authorized persons
- if there is a simple need for the site to remember you between visits and adapt itself to your needs or wishes
- to allow you to receive further information that you have requested, such

as newsletters and information updates

- to grant you individual privileges that you might request or you may be entitled to otherwise.

We store the information that you provide on the registration form (if you register yourself) or that your organization provides directly to us. **The information you provide may be made available to the sites other than the one for which you originally obtained the account provided that you attempt to access them while logged in using your account.** By logging in and accessing accounts you are indicating your consent to the use of the data as described in this statement.

The data obtained from the registration process includes personal details and details related to your link with that organization if you are registered as a representative, or member of an organization. Personal details include your full name, your geographical location, your areas of interest (with respect to the Company), your e-mail address and your telephone number. If you are a member of an organization, the details may include the organization's name, the department you work for, your office address, the nature of your relationship with that organization (e.g. employee), your role and job title and, in order to avoid creating duplicate records, a unique identifier. Information that is obtained from your organization is subject to the regulations concerning the transfer of personal data and may be only a subset of that mentioned.

The account that we create contains enough information for us to have reasonable confidence that its subsequent usage is by yourself, or by someone who is authorized to have access to the information you provided (including the password).

We also store certain additional information (listed below) relating to the activity on the user account that we create for you, so that we can protect both your identity and the integrity of the Company systems that you access.

The additional information is used to diagnose and resolve problems and to deal with security incidents. Much of it relates to attempts to use an identity and thus to events that occur before a user has successfully authenticated.

The Identity Management Service also stores a list of the access rights granted to you by the Company for the purpose of granting or denying access to individual sites.

Users can inspect all the data that is maintained about their own account, allowing them to check that their account has not been used, and that attempts

have not been made to use it, without their knowledge and consent.

We may collect the following additional data about each user:

- Date and time of
    - most recent successful and unsuccessful authentication
    - last change of password
    - last password reset
- Number of good logins and failed attempts
- Your most recent passwords - to make sure you follow the prevailing security policy regarding password re-use.

When you login and / or change your password, we may record further information in log files, such as the IP address used, in line with the purposes stated above. This information can help in following up any doubtful activity relating to your account. It will **not** be used to monitor your activity, except to allow the removal of the account when no longer used.

3. Who would have access to your information and to whom would it be disclosed?

By registering yourself, you authorize the disclosure of the details you have entered in the user registration system to any site that you access after having given your email address and password. If you were registered by your organization, your consent is presumed to have been given (implicitly) for the transfer of your personal information.

The details of the activity associated with your account are never passed on to any other company site by The Modern.Press.

The Company will not divulge your information to the third parties outside the The Modern.Press with the following exceptions:

- the duly authorized support unit, or help desk responsible for the domain in which you are registered
- duly authorized entities for the purpose of preserving your privacy, you can choose (through an option on the log-in screen) to be notified whenever a relying party requests your identity - you will have the option to cancel the operation before any information is passed on. Beware that this may render the application inaccessible to you. If, having logged in into EU Login, you wish to access sites anonymously, you can do one of the following before connecting to the site in

question:

open a new browser session and use it to access the site;

log out from the authentication service; or

disable cookies in your browser options.

Note that behavior varies from one browser to another, and may affect the results of these operations.

If you need to access the site that requires you to register and authenticate, but you do not wish it to have access to the details you supplied in order to gain access to another Company's site, we suggest you create a separate account for this purpose. This will require you to provide a distinct e-mail address, which need not be traceable to you personally. Of course, this may deny you access to certain sites which require proof of identity.

Your password is stored only in an irreversible form. Apart from your password, the service administrators can view all of the data pertaining to a particular user. This helps them to perform duties such as helping users with problems and diagnosing suspicious security incidents.

4. How do we protect and safeguard your information?

The Company stores your personal information in secure computers and your information may only be accessed by authorized persons and through internal sites.

When you log in, the password is always encrypted on the network and is decrypted for checking against the stored password by the authentication service, not by the individual site. All passwords (including previous passwords mentioned above) are stored in a form that permits them to be checked against a supplied value, but their actual value cannot be derived from the stored value.

The details about your user account are available only to yourself, and to the service administrators.

If you registered yourself directly, you should be aware that anyone with access to read your e-mail may be able to use the account you created and acquire the

identity it represents. You are personally responsible for assessing the risk that this presents to you.

Furthermore, certain users are allowed to reset their password using e-mail. They should bear in mind that anyone else with access to their e-mail (because of automatic forwarding, delegation or for other reasons) will be able to reset the password.

For this reason, in order to perform important business or access sensitive information, the Company requires more stringent identity checks and your account will need to be set up or transformed specifically for this purpose. You will need to contact the relevant Company department or a delegated representative in your organization to achieve this.

If you have any reason to believe that your password has been compromised – for example, if your password appears to have been changed without your knowledge - you should notify your normal support contact or contact the Company as described on the user registration and authentication pages.

Notes:

In principle, and especially if you have access to sensitive systems, you should never reveal your password to anybody else: it must be kept as a secret. In particular, your Login password should only ever be entered on screens showing the approved Login logo. Do not enter it if you are suspicious about the authenticity of the Login site.

When you enter your password, make sure your browser indicates (usually by means of a padlock or other icon) that you are on a secure connection, and that you are connected to a Company site address.

5. How can you verify, modify or delete your information?

You can verify your account information, including the data recorded about activity on your account, in the pages of either the user registration service or through the authentication service (“Login”). This excludes information that is only held in log files: if you wish to access your log file entries, you may request it by writing to the Controller at the address given below. A response will be given within a period of six weeks from the date of receipt of the request.

In case of difficulty, you can obtain help by following the contact link below (see point 7).

If you registered yourself in the Company's system, you will be able to change or

remove any personal information on-line. However, if your details were registered through a Third Party, this may not be possible and you will have to contact that Third Party in order to have the information changed: you may nevertheless have the information removed by the Company, but if the Third Party re-submits this information to the Company, it will be re-instated.

Since it is collected automatically, it is not possible to modify any of the technical data held by the authentication service, with the exception of the password itself.

6. How long do we keep your data?

The Identity Management Service keeps your data for as long as you are recorded as an active user, and for a period of one year thereafter. Data concerning users automatically registered from internal sources may be kept for as long as it is retained in the source system. If you were registered through a Third Party, the period of activity will usually correspond to a contractual link with that party or be subject to an expiration date. In other cases, the Company will consider you active as long as you continue to use your account or until your account expires.

Note that in the case of users who registered with IMS themselves, the period of one year is extended in order to allow the exchange of e-mail with a user. This exchange will provide for the user to request an extension, thus resetting to zero the recorded period of inactivity. In the absence of a response from the user, all personal data will be deleted.

Data from the Identity Management Service is backed up regularly by the Company to ensure a correct system restore if necessary to restart operations. Furthermore, the Identity Management Service is closely monitored and all sensitive actions on the system are logged, including each authentication request. These logs (log files) are rotated regularly and removed from the active system after a maximum of six months in accordance with REGULATION (EU) 2018/1725. All log files backed up by the standard Company's backup procedure will not be removed from back-up tapes until those tapes are recycled, but that log data will not be restored if system restore is required.

7. Contact Information

If you wish to ask questions or post complaints about the service with respect to the use of your personal information, you should follow the contact link that is shown on each Identity Management service page, or write to the following address:

https://www.themodern.press/gdpr

8. Recourse

If necessary, complaints can be addressed to the European Data Protection Supervisor.

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") forms part of the Contract forServices ("**Principal Agreement**") between

_____

(the "**Company**") and

_____(t
he "Data Processor")

(together as the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "Contracted Processor" means a Sub-processor;

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent

applicable, the data protection or privacy laws of any other country;

1.1.5 “EEA” means the European Economic Area;

1.1.6 “EU Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 “GDPR” means EU General Data Protection Regulation 2016/679;

1.1.8 “Data Transfer” means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 “Services” means the 'data-management' services the Company provides.

1.1.10 “Sub-processor” means any person appointed by or on behalf of Processor to process

Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1. comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company’s documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the

Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory confidentiality obligations.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Sub-processor unless required or authorized by the Company.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Company obligations, as reasonably understood by the Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 ***Processor shall;***

6.2.1 promptly notify the Company if it receives a request from a Data Subject under any Data Protection Law regarding the Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of the Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform the Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify the Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting the Company Personal Data, providing the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Company reasonably considers to be required under Article 35 or 36 of the GDPR, or under equivalent provisions of any other Data Protection Law, in each case solely regarding Processing of the Company Personal Data by, and taking into account the nature of the Processing and information available to the Contracted Processors.

9. Deletion or return of the Company Personal Data

9.1 Subject to this section 9, a Processor shall promptly and in any event within ten (10) business days of the date of cessation of any Services involving the Processing of Company Personal Data (the “Cessation Date”) delete and procure the deletion of all copies of the related Company Personal Data.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for, and assist in audits, including inspections, by the Company or an auditor mandated by the Company regarding the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise provide them information and audit rights meeting the relevant requirements under the Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without a prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the

personal data would be adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on the EU recognized standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose this Confidential Information without the **prior written consent** of the other Party except to the extent that:

(a) disclosure is required by law; or

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be either delivered personally; sent by registered mail with a return receipt, sent by email to the address provided; emailed to the address set out in the heading of this Agreement; or mailed to such other address as provided from time to time by the Parties who would have a change of address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of England and Wales

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of London, subject to possible appeal to Supreme Court of London.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Company

Signature _____

Name:_____

Title:_____

Date Signed: _____

Processor Company

Signature_____

Name_____

Title _____

Date Signed _____

COOKIES POLICY

What are cookies?

A cookie is a small text file that a website stores on your computer or mobile device when you visit the site.

First party cookies are cookies set by the website you're visiting. Only that website can read them. In addition, a website might potentially use external services, which also set their own cookies, known as third-party cookies.

Persistent cookies are cookies saved on your computer and that are not deleted automatically when you quit your browser, unlike a session cookie, which is deleted when you quit your browser.

Every time you visit the Commission's websites, you will be prompted to accept or deny access to cookies.

The purpose is to enable the site to remember your preferences (such as user name, language, etc.) for a certain period of time.

That way, you don't have to re-enter them when browsing around the site during the same visit.

Cookies can also be used to establish anonymous statistics about the browsing experience on our sites.

How do we use cookies?

European Commission websites mostly use "first-party cookies". These are cookies set and controlled by the Commission, not by any external organization.

However, to view some of our pages, you will have to accept cookies from external organizations.

The 3 types of first-party cookie we use are to:

- store visitor preferences
- make our websites operational
- gather analytic data (about user behavior)

Visitor preferences

There are no cookies that we can reach and determine; in other words, cookies

for Visitors are not used.

Operational cookies

There are some cookies that we have to include in order for certain web pages to function. For this reason, they do not require your consent. In particular:

- authentication cookies;
- technical cookies required by certain IT systems

Authentication cookies

These are stored when you log in to the site, using our authentication service (Login). When you do this, you accept the associated privacy policy automatically.

Name: tmp_user_id, stmp_user_email

Service: TheModern.Press

Purpose: These cookies are used for Authentication process

Cookie type and duration: First-party session cookie. If the user has selected “remember me”, it will be deleted after 54 years, if not ~~than~~ then it will be deleted 1 hour after turning off the browser.

Technical cookies

Name: tmp_feed_views

Service: TheModern.Press

Purpose: cookie that keeps track of what news is being viewed

Cookie type and duration: First-party session cookie. Cookie will be deleted 1 hour after **turning off** the browser.

Analytics cookies

We use these purely for internal research for purposes of improving the service

we provide for all our users.

The cookies simply assess how you interact with our website – as an anonymous user (the data gathered does not identify you personally).

Also, this data is not shared with any Third Parties or used for any other purposes. The anonymous statistics could be shared with contractors working on communication projects under a contractual agreement with the Commission.

However, you are free to decline these types of cookies – either via the cookie banner you'll see on the first page you visit, or at https://www.themodern.press/gdpr

We use Google Analytics cookies to collect information on how visitors use our website. These cookies collect information in the aggregate to give us insight into the means our website is being used. The IP addresses shall be anonymous in Google Analytics, and this anonymous data is transmitted to and stored by Google on servers in the United States. Google may also transfer this information to the Third Parties where mandated by law, or where such Third Parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. The following table has more information about these cookies.

Cookie Name	**Source**	**Expiry**	**Purpose**	**How to Block**
_ga	Google Analytics	2 years from set/update		

These cookies are used to collect information on how visitors use the ENAEE website. We use the information to help us improve our site through the collection of anonymous information

Open the Cookie Consent Tool to set your preferences or, delete these cookies through your browser settings.

Cookie Name Source Expiry Purpose How to Block

_ga	Google Analytics	2 years from set/update	These cookies are used to collect information on how visitors use the ENAEE website. We use the information to help us improve our site through the collection of anonymous information (e.g., number of visitors to website and where visitors have come to the site from).	Open the Cookie Consent Tool to set your preferences or delete these cookies through your browser settings.
_gid	Google Analytics	24-hours		
_utma	Google Analytics	2 years from set/update		
_utmz	Google Analytics	6-months from set/update		

To view an overview of the privacy of Google Analytics cookies please go here:

https://support.google.com/analytics/answer/6004245.

You may install a Google Analytics Opt-out Browser Add-on by going here: https://tools.google.com/dlpage/gaoptout.

Third-party cookies

There is no display content from external providers on our pages.

How can you manage cookies?

You can delete all cookies that are already on your device by clearing the browsing history of your browser.

Removing cookies from your device

You can delete all cookies that are already on your device by clearing the browsing history of your browser.

This will remove all cookies from all the websites you have visited.

Managing site-specific cookies

For more detailed control over site-specific cookies, check the privacy and cookie settings in your preferred browser

Blocking cookies

You can set most modern browsers to prevent any cookies being placed on your device, but you may then have to manually adjust some preferences every time you visit a site/page. And some services and functionalities may not work properly at all (e.g. profile logging-in).

Managing our analytic cookies

You can manage your preferences concerning cookies from Europa Analytics on the dedicated following pages.

To view an overview of the privacy of Google Analytics cookies please go here:

https://support.google.com/analytics/answer/6004245.

You may install a Google Analytics Opt-out Browser Add-on by going here: https:// tools.google.com/dlpage/gaoptout.