

PRIVACY POLICY

LAST UPDATED 18 JUNE 2019

1. Who we are

EUNOMIA (“we” or “us”) is an EU funded project (Grant Agreement no: 825171) that began 2018 and ends in 2021. The EUNOMIA consortium partners, as listed [here](#), are joint data controllers responsible for the collection and use of your personal information. For further information, we can be contacted at eunomia@gre.ac.uk.

2. Scope of this Privacy Notice

This Privacy Notice aims at informing website visitors, our partners, and other stakeholders about how we process personal data. We are committed to processing personal data responsibly, securely, and proportionally throughout our activities.

3. How we collect your personal data

We collect personal data both directly and indirectly from individuals including:

Directly. We obtain personal data directly from individuals in a variety of ways, including but not limited to obtaining personal data when:

- you subscribe to our newsletter/s
- register to attend meetings and events we host and during your attendance at such events
- visit the offices of our partners
- when we are establishing a research relationship
- when we are performing professional services pursuant to our contract with the European Commission
- you participate in a form or survey for the purpose of research activities that we perform either independently or in collaboration with you

Indirectly. We obtain personal data indirectly about individuals from a variety of sources, including:

- our research partners
- our networks and contacts
- public and open data sources such as public registers (e.g., Companies House), news articles and internet searches
- social and professional networking sites (e.g., LinkedIn)

4. The personal data types we collect

We collect the following types of personal data about individuals, including:

General personal data types, including:

- Contact details (e.g., name, affiliation, job title, work and mobile telephone numbers, work and personal email and postal address)
- Personal information (e.g., age, gender, nationality) that is collected for research purposes to understand how these characteristics influence a particular research area

Special categories of personal data, which we collect with explicit consent, including:

- Dietary restrictions and identification documents when registering for in-person events that may reveal religious beliefs or health preferences
- Expense forms submitted for internal reimbursement from attendance at events that include bank account information
- Sensitive personal data (e.g., political opinions) may be collected during our research to understand the social and political considerations in the verification of social media information. If collected, this data will be processed in a manner that does not affect your individual rights and that will protect your identity. We will anonymise the data you provide us to the extent possible.

5. The lawful bases for processing your personal data

We process personal data on the following bases:

- *Consent* – when you provide us with your personal data directly, for example when you subscribe to our newsletter
- Legal obligations – We may process personal data in order to meet any legal obligation requiring us to do so, e.g., reporting to the European Commission
- Legitimate interests– We process personal data when it is necessary for us to achieve the following legitimate interests:
 - *Enhancing our research delivery; and*
 - *Undertaking dissemination activities*

6. What we do with your personal data

We process your personal data with the purpose of:

- Conducting research (e.g., interviews, surveys)
- Promoting our research to different types of stakeholder
- Sending invitations and providing access to guests attending our events and webinars
- Administering, maintaining and ensuring the security of our information systems, applications and websites
- Processing online requests or queries, including responding to communications from individuals
- Complying with legal and regulatory obligations

7. How we secure your personal data when we process it

We have put appropriate technical and organisational security policies and procedures in place to protect personal data (including sensitive personal data) from loss, misuse, alteration or destruction. We aim to ensure that access to your personal data are password protected. We encrypt all data stored at our central location and data are restricted only to those who need to access it. Those individuals who have access to the data are required to maintain the confidentiality of such information. We install and regularly update all security and anti-virus software in use on all of our systems. Please be aware that the transmission of data via the Internet is not completely secure. Whilst we do our best to try to protect the security of your personal data, we cannot ensure or guarantee the security of your data transmitted to our site.

8. Do we share personal data with third parties?

We may occasionally share personal data with trusted third parties to help us deliver efficient and quality services. When we do so, we ensure that recipients are contractually bound to safeguard the data we entrust to them before we actually share the data. We may engage with several or all of the following categories of recipients:

- Parties that support us as we provide our services (e.g., cloud-based software services such as Dropbox, Microsoft Sharepoint)
- Our professional advisers, including lawyers, auditors and insurers
- Payment services providers
- Marketing services providers (e.g., MailChimp)
- Law enforcement or other government and regulatory agencies (e.g., HMRC) to report crime or to other third parties as required by, and in accordance with applicable law or regulation
- The European Commission auditors for reporting purposes when we are required by them to do so in relation to our work with them on EC funded H2020 projects

9. Do we transfer your personal data outside the European Economic Area?

We store personal data on servers located in the European Economic Area (EEA) and outside of the EEA, namely the US. We transfer personal data to reputable third-party service providers, namely SharePoint, DropBox, MailChimp, situated both inside and outside the EEA. Please refer to their websites for further information about their personal data handling. Each organisation is required to safeguard personal data in accordance with our contractual obligations and data protection legislation.

10. Do we use cookies?

Our website does use cookies. Where cookies are used, a statement will be sent to your browser explaining the use of cookies. To learn more, please refer to our cookie policy.

11. Your data protection rights

You have the following rights in relation to your personal data that we process. You can exercise your rights by emailing us at compliance@greenwich.ac.uk, including:

- Right to Withdraw Consent– You can withdraw your consent that you have previously given to one or more specified purposes to process your personal data. This will not affect the lawfulness of any processing carried out before you withdraw your consent. It may mean we are not able to provide certain products or services to you and we will advise you if this is the case.
- Right of access– You can ask us to verify whether we are processing personal data about you, and if so, to have access to a copy of such data
- Right to rectification and erasure– You can ask us to correct our records if you believe they contain incorrect or incomplete information about you or ask us to erase your personal data after you withdraw your consent to processing or when we no longer need it for the purpose it was originally collected
- Right to restriction of processing– You can ask us to temporarily restrict our processing of your personal data if you contest the accuracy of your personal data, prefer to restrict its use rather than having us erase it, or need us to preserve it for you to establish, exercise, or defend a legal claim. A temporary restriction may apply while verifying whether we have overriding legitimate grounds to process it. You can ask us to inform you before we lift that temporary processing restriction
- Right to data portability– In some circumstances, where you have provided personal data to us, you can ask us to transmit that personal data (in a structured, commonly used, and machine-readable format) directly to another company
- Right to Object – You can object to our use of your personal data for direct marketing purposes, including profiling or where processing has taken the form of automated decision making. However, we may need to keep some minimal information (e.g., email address) to comply with your request to cease marketing to you
- Right to make a complaint to the UK Information Commissioner's Office (<https://ico.org.uk/concerns/handling/>) regarding any concerns you may have about our data handling practices.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information or to exercise any of your other rights. This helps us to ensure that personal data is not disclosed to any person who has no right to receive it. No fee is required to make an initial request unless your request is clearly unfounded or excessive. Depending on the circumstances, we may be unable to comply with your request based on other lawful grounds.

12. How long do we retain personal data?

We retain personal data to provide our services, stay in contact with you and to comply with applicable laws, regulations and professional obligations that we are subject to. Unless a different time frame applies as a result of business needs or specific legal, regulatory, or contractual requirements, we retain personal data for

a period of 12 months after the research project ends. However, please note that we have an obligation to retain data concerning European Union research projects (H2020, Action Grants, FP7, etc.) for up to 10 years after the end of the project (unless further retention is requested by auditors), and the retention period of HMRC-related data, which is 7 years.

As the records and documentation containing personal data have been collected within the delivery of an EC project, the Commission/Agency will process it in compliance with Regulation No 45/2001 (archived for at least 5 years after the balance is paid unless there are ongoing procedures such as audits, investigations or litigations, in which case the evidence must be kept until these end, even if this is longer than five years). After the expiry of the retention period, and unless further legitimate grounds for retention arise, we will dispose of personal data in a secure manner.

13. Do we link to other websites?

Our websites may contain links to other sites, including the sites of the consortium partners that are not governed by this Privacy Notice. Please review the destination websites' privacy policies before submitting personal data on those sites. Whilst we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content, security, or privacy practices employed by other sites.

14. Do we change this Privacy Notice?

We regularly review this Privacy Notice and will post any updates to it on this webpage. This Privacy Notice was last updated 18 June 2019.

15. Contact us

If you have any concerns as to how your data is processed, you can contact us per email or per post:

Data Protection Officer, University Secretary, University of Greenwich, Queen Anne Court, Old Royal Naval College, Park Row, Greenwich, SE10 9LS or at compliance@greenwich.ac.uk.

We will respond to your queries within 30 days from when we receive them.