

EUROCRIME PRIVACY POLICY – GDPR

INGLESE

Privacy Policy

1

Welcome to EuroCrime's Privacy Policy

Personal data provided by you on www.eurocrime.eu, other EuroCrime's owned and controlled websites and EuroCrime's newsletter submission system is processed by EuroCrime – Research, Training and Consulting Srl, Nicolò Machiavelli St., 52, 50026, San Casciano in Val di Pesa (Florence), Italy (hereinafter referred to as the '**Controller**' or '**We**') in a confidential manner, in compliance with the provisions herein and the prevailing privacy laws, including the Reg (EU) 2016/679 (GDPR).

FIELDS OF PROCESSING YOUR PERSONAL DATA

Newsletter

If you wish to receive useful information on EU funding opportunities, tips for proposal development and project management, information about the EU funding world, security and criminology issues, Ethics and data protection, and stay informed about our activities, researches, trainings and ongoing projects, you can subscribe to our newsletter via the website. You can unsubscribe from the newsletter any time, with no charge applied.

The purpose of data processing: Sending of an electronic newsletter - provision of information on EU funds, calls for proposals, news, events and projects, security and criminology issues, Ethics and data protection and all the EuroCrime's activities, in an electronic newsletter.

The scope of the data processed: Name, Email Address.

The legal basis of data processing: The consent of the Data Subject.

The term of data processing: Until the cancellation of your subscription to the newsletter, but maximum 10 years.

Customer Service

If you have any questions regarding our services, research and training opportunities, consultancy services, you can contact the Controller at the contact details provided herein, or on the website, or under the Contact Details page of the website, or by completing the contact form provided therein.

The purpose of data processing: The handling of questions and other issues related to EuroCrime's services and activities, i.e. training courses, conferences, research activities, consultancy services.

The scope of the data processed: Name, Email Address.

The legal basis of data processing: The consent of the Data Subject.

The term of data processing: 10 years.

Website visitor data

Anyone can access EuroCrime's website (without a need for identification, or to supply personal data), and can gain information from there, or from any related websites, freely and without any restrictions applied. However, the website automatically collects general (not tied to the individual visitors' person) information about the website visitors, in an unrestricted manner. Nonetheless, no such data allows the website operator to gain any personal information about the visitors.

The purpose of data processing: When visiting the website, the service provider records visitor data, for the purposes of monitoring the operability of services, facilitating and enhancing the website functions, and providing and individuated customer service, and for the prevention of abuse.

The scope of the data processed: date, timing, website address, any subpages previously visited on the Website, data related to the user's operating system and web browser, the operating system used, and the user's IP address, except for the last few digits.

The legal basis of data processing: the legitimate interest of the Controller (for the above-mentioned purposes).

The term of data processing: 7 days. In addition, the data will only be stored if it is necessary to investigate detected attacks on the website.

Cookies

To make this Website work properly, we sometimes place small data files called cookies on your device. Most big websites do this too.

What are cookies?

A cookie is a small text file that a website saves on your computer or mobile device when you visit the site. It enables the website to remember your actions and preferences (such as login, language, and font size and other display preferences) over a period of time, so you don't have to keep re-entering them whenever you come back to the site or browse from one page to another.

How do we use cookies?

- We use cookies that are strictly necessary to enable you to move around the site or to provide certain basic features.
- We use cookies to enhance the functionality of the website by storing your preferences, for example: language.
- We also use cookies to help us to improve the performance of our website to provide you with a better user experience.

The following 3rd-party cookies are also used on our pages:

- **Youtube (embedded videos):** PREF, VISITOR_INFO1_LIVE, YSC
- **Google Analytics:** __utma, __utmb, __utmc, __utmz, __utmv
- **LinkedIn policy:** <https://www.linkedin.com/legal/cookie-policy>
- **LinkedIn (configuration):** <https://www.linkedin.com/settings/>

Enabling these cookies is not strictly necessary for the website to work but it will provide you with a better browsing experience. You can delete or block these cookies, but if you do that some features of this site may not work as intended.

Do we use other cookies?

Some of our pages or subsites may use additional or different cookies to the ones described above. If so, the details of these will be provided in their specific cookies notice page. You may be asked for your agreement to store these cookies.

How to control cookies

You can **control and/or delete** cookies as you wish – for details, see AllAboutCookies.org. You can delete all cookies that are already on your computer and you can set most browsers to prevent them from being placed. If you do this, however, you may have to adjust manually some preferences every time you visit a site and some services and functionalities may not work.

Transmission of data

The Controller may disclose personal data to any official authorities (provided that such authorities have clearly indicated the exact purpose, and the scope of data required), for legal/juridical reasons and if this is necessary to fulfil the purposes indicated for such request.

Data Security

The Controller and the data processor(s) shall handle all personal data in a confidential manner and observe the prevailing data protection laws and regulations, and in the Strasbourg Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and Regulation (EU) 2016/679 of the European Parliament and of the Council 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).

In order to ensure the safe processing of data, the Controller shall take all IT and other measures related to the storage, processing, and transmission of data. The Controller shall take the expectable measures to protect the personal data processed by it against unauthorized use, alteration, disclosure, deletion, damage or destruction and to ensure the technical conditions required thereto.

The persons entitled to have access to data

The data provided by you will be available only for those employees and agents of the Controller, the performance of whose tasks and duties require the knowledge of such data.

Your rights, as Data Subject

The aim of this information is to provide proper information on facts and particulars related to data processing for the Data Subjects (hereinafter referred to as the **'Data Subject'**), already prior to the commencement thereof.

You are entitled to obtain confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and to the following information:

1. the purposes of data processing;
2. categories of the affected personal data;
3. the recipients or categories of recipient to whom eventually the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5. the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the Data Subject or to object to such processing;
6. the right to lodge a complaint with a supervisory authority;
7. where the personal data are not collected from the Data Subject, any available information as to their source;
8. the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

Upon request, the Controller shall provide you with a copy of the personal data undergoing processing.

You may request at any time the correction or supplementation of erroneous personal data; the Controller shall take the requested measures without undue delay.

You are entitled to withdraw your consent at any time.

The consent may be withdrawn by using the adequate link or by sending your request for the withdrawal of your consent to the Controller, as described herein.

The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

In case you withdraw your consent, the Controller shall delete your personal data from their database within 30 days.

Upon the request of the Data Subject, the Controller shall delete the personal data concerning him or her, without undue delay, if

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the Data Subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;
- the processing of the personal data is for direct marketing purposes, and the Data Subject objects to the processing, and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed; or
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller are subject.

Where the Controller have made the personal data public and are obliged pursuant to the present section to erase the personal data, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform Controller which are processing the personal data that the Data Subject has requested the erasure by such Controller of any links to, or copy or replication of, those personal data.

The above provisions shall not apply to the extent that processing is necessary:

- a. for exercising the right of freedom of expression and information;
- b. for compliance with a legal obligation which requires processing by Union or Member State law to which the Controller are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- c. for reasons of public interest in the area of public health;
- d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to deletion is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- e. for the establishment, exercise or defence of legal claims.

The Controller shall restrict data processing upon the request of the Data Subject, if

- the accuracy of the personal data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the personal data;
- the processing is unlawful, and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Controller no longer need the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
- if the processing of personal data takes place for direct marketing purposes and the Data Subject has objected to processing; in this case, the restriction shall be valid as long as it is verified whether the legitimate grounds of the Controller override those of the Data Subject.

Where processing has been restricted according to the above, such personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. The Controller shall inform a Data Subject, who has obtained restriction of processing pursuant to the above provisions, before the restriction of processing is lifted.

In addition to the above, the Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided.

Requests may be submitted addressed to: EuroCrime SrL – Niccolò Machiavelli St., 52, 50026, San Casciano in Val di Pesa (Florence), Italy via post, or to info@eurocrime.eu via e-mail.

For the sake of identification, correct and specific personal data shall be provided.

The Controller shall notify the Data Subject of the measures taken upon the request for exercising his/her rights without undue delay, but in any case, within 30 days of the receipt of the request.

Where the Data Subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

The correction, restriction, and deletion of data shall be reported by the Controller to the concerned Data Subject and those, to whom the affected data were previously transmitted for data processing purposes.

The Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her, which is based on a legitimate interest. In such a case, the Controllers may no longer process the personal data unless the Controllers demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

The Controllers shall suspend the data processing and examine the objection within the shortest possible deadline, but within maximum 30 days and inform the requesting party of the result thereof in writing. If the objection is well-grounded, the Controllers shall terminate the processing (including any further collection or transmission of data) and shall restrict the affected data. Furthermore, the Controllers shall notify of the objection and the measures taken in response thereto those, to whom the personal data affected by the objection were transmitted previously; these recipients shall also provide for the enforcement of the right to object.

If the Controllers do not take action on the request of the Data Subject, the Controllers shall inform the Data Subject without delay and at the latest within 30 days of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

In case of infringement of the above-mentioned rights, you may turn to a court or the Italian National Authority for Data Protection and Freedom of Information (Italian DPA – Garante per la Protezione dei Dati Personali,).

Italian National Authority for Data Protection and Freedom of Information (DPA):

Address: Piazza di Monte Citorio, 121 – 00186 Roma, Italy

Phone: +39-06-6967 71

Fax: +39-06-6967 73785

www: http://www.garanteprivacy.it/home_en

e-mail: garante@gpdp.it

EuroCrime Privacy Policy, effective date 25 May 2018