BLUEMED PROJECT PRIVACY POLICY

BlueMed Project Portal takes your privacy seriously and treats all the personal data with great care. We are committed to protecting your privacy and will only use the information that is collected about you lawfully. This policy is intended to give you an understanding of how and why we use the personal information you give us or we receive from others according to the General Data Protection Regulation (EE 2016/679) ''GDPR''.

In this Privacy Policy we describe how we collect, process, share and protect your data. We also describe why we process your personal data and the associated choices and rights you have with regards to your personal data.

Who is responsible for the processing of your personal data?

ATLANTIS CONSULTING S.A. is the Data Controller and responsible for the processing of your data.

ATLANTIS CONSULTING S.A.

47 Steliou Kazantzidi Str.

570 01 Pylaia | Thessaloniki Greece

Tel.: (+30) 2310 53 10 00

Fax: (+30) 2310 55 22 65

For more information on this company please contact info@atlantisresearch.gr

Why we collect Personal Data

We collect personal data information to provide advice, to provide goods and services, to fundraise or to undertake research, as well as to send newsletters in order to inform our members about relative projects and other actions.

Personal Data we collect

We collect only the personal data needed for the purposes of the portal. These data may refer to personal information (including name, email, address, phone number), or information about people we advise, owners, agents and other parties with an interest in our field including but not limited to supporters, applicants, volunteers and employees.

Personal data protection principles

When we process personal data, we are guided by the following principles, which are set out in the GDPR. We are responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

1. processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency).
2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation).
4. accurate and where necessary kept up to date (Accuracy).
5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).
6. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality).

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. where the legal basis of our processing is Consent, to withdraw that Consent at any time
2. to ask for access to the personal data that we hold
3. to prevent our use of the personal data for direct marketing purposes
4. to object to our processing of personal data in limited circumstances
5. to ask us to erase personal data without delay:

a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed
b. if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data
c. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest
d. if the data subject has objected to our processing for direct marketing purposes
e. if the processing is unlawful.

6. to ask us to rectify inaccurate data or to complete incomplete data
7. to restrict processing in specific circumstances e.g. where there is a complaint about accuracy
8. to ask us for a copy of the safeguards under which personal data is transferred outside of the EU
9. the right not to be subject to decisions based solely on automated processing, including profiling
10. to prevent processing that is likely to cause damage or distress to the data subject or anyone else
11. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms

12. to make a complaint to the Privacy Authority and
13. in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. another portal) in a structured, commonly used and machine-readable format.

Accountability

The portal must implement appropriate technical and organizational measures in an effective manner to ensure compliance with data protection principles. The portal is responsible for, and must be able to demonstrate compliance with, the data protection principles.

Responsibilities

As the Data Controller, we are responsible for establishing policies and procedures in order to comply with data protection law.

Reporting a personal data breach

The GDPR requires that we report to the Privacy Authority any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialize, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the Authority where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, you should immediately contact us at info@atlantisresearch.gr and follow the instructions in the personal data breach procedure. You must retain all evidence relating to personal data breaches in particular to enable the University to maintain a record of such breaches, as required by the GDPR.