

PRIVACY POLICY OF THE APPLICATION Drop A Message

The purpose of this document is to inform you about the sort of personal data that EYDAP S.A. is collecting through the application Drop A Message [hereafter the “Application”], as Controller, the way of its processing (collection, storage, use, transfer etc.), the purpose of its processing, the technical and organizational measures aiming at its protection and the rights that users hold over this processing, which in any event is being realized in a reliable, legal and transparent way, in compliance with the provisions of the General Data Protection Regulation [EU 2016/679], the Greek legislation [Law 4624/2019] and the related acts of the Hellenic Data Protection Authority, Law 3471/2006, as they currently stand about the protection of natural persons with regard to the processing of personal data.

1. Which information we collect and for which purposes /legal bases

The information collected upon the installation of the Application includes: the email address, the serial number of the activation of the Application, the Universally Unique Identifier (UUID) of the device, the name and version of the operating system installed on the device, the IP address of the user. The keeping of the aforementioned data is necessary for reasons of computer system safety [article 6, paragraph 1, point f) of GDPR].

It must be noted that each provider of app store services (Apple App Store or Google Play) is automatically processing, upon loading our Application, your personal data. At that time, EYDAP is not collecting data nor is it associated in any way with the collection of it. For more information, you can refer to the corresponding Privacy Policies of Google Play Store:

<https://policies.google.com/privacy?hl=el&gl=el> and Apple App Store:

<https://www.apple.com/legal/privacy/en-ww/>

Upon registration to the Application, users provide EYDAP with their email and create a username. This user information is necessary for identification and creation of a unique account. The username for labelling the username to other users when a user sends them a private message. The information that a user writes in the content of the bottle and announces to other users is controlled by content by the Controller of the Application in order to avoid offensive and non-lawful behaviours upon use of the Application and in breach of its operating rules. [see Terms of Use].

When using the Application, your current location might be specified via GPS technology (or other similar), in order for the device to identify the area where you are for the display of related messages/ data/ adapted operations. The location of users is not uploaded into the database of the Application nor is it stored somewhere, but is used by the Application locally in the device, only to allow users to “get connected” to a Well of Hadrian’s Aqueduct, if there is one nearby, in order to lift, see, drop bottles.

EYDAP collects and processes your data only when you proceed with the downloading and use the Application, with your consent [article 6, paragraph 1, point a) of GDPR].and following the acceptance of the Terms of Use and the present Privacy Policy.

Personal data is provided freely by users or is automatically obtained when this Application is being used, following prior notification and consent by users. The data collected by this Application are used for the identification of the users and the storage of their preferences, aiming exclusively at the provision of the service required upon use. Failure to provide some personal data may make the provision of the services of the Application impossible.

For reasons of operation and maintenance, the Application may collect files that are recording anonymous information regarding the use of the Application (record-oriented file system).

It is possible to collect information in an anonymized form exclusively for statistical purposes [for instance, how many users have connected to the Application]. This information is not in any way used for the identification of visitors/users.

2. How we share the information we collect

EYDAP will not in any way exploit your information and personal data or transfer those to third parties, except when this is imposed or allowed by each legal framework in force.

In particular, access to your data is granted to the authorized personnel of our Company [hereafter the “Controller” of the Application], which is bound by confidentiality clauses in order to safeguard the privacy of your data.

In particular, the personal data of users can be used for legal purposes by EYDAP, being the Controller, before courts, prosecution offices or other competent authorities in potential legal proceedings that might arise due to inappropriate or/and non-lawful use of this Application or the related services. In this event, users are informed via the present Policy and state that they are aware that the Controller may be obliged to reveal their personal data in case this is required by the aforementioned public authorities, within the framework of the lawful obligations of the Company, protection of its rights and properties, the other users of the Application and in general the exercise of the legal claims of the Company.

Where applicable, your personal data is communicated to third parties (natural or legal persons) collaborating with us, when deemed necessary for the fulfilment of the contractual obligations of the Company and the provision of the agreed services to you and/or the fulfillment of the obligations of the Company, arising out of the legislative framework in force.

Moreover, in order to provide you with our services, EYDAP uses the services of Firebase Database [google.firebase.com], which acts on behalf of us [as Processor] by providing us with the following individual services:

- Firebase Authentication (for registration/entry of the end user)
- Cloud Storage for Firebase (for storage in the cloud of .JSON files that include the ready-to-use messages of EYDAP. The end users do not store data in this service; they just read).
- Firebase Realtime Database (for storage and readout of user data and messages in a bottle in real time).
- Firebase Analytics (for the Controller of EYDAP to view detailed forms with statistics of the Application, where anonymous information is being collected by Firebase – for instance, “total number of active users of the Application on iOS and Android).

Regarding the use the aforementioned services and the data that Google is collecting from the end users of Firebase, that are similar to the data collected by all the applications of Google from the devices of users, in detail <https://policies.google.com/technologies/partner-sites> and <https://www.termsfeed.com/blog/firebase-privacy-policy/> and include among others: 1. Information about the device of the user, 2. Information about the use of the application (e.g. time that the Application is open), 3. Android Ad ID or Apple Identifier for Advertisers (IFDA). As you have been informed above, throughout the use of the Application, general information, that is collected for all Firebase applications, is automatically collected

anonymously (hours of use, geographical distribution per country etc.), as well as information about how many times the users have opened, on average, each page of the Application, in order to publish anonymous statistical data.

Excluding the processing by Google Firebase, as described above, we do not transfer your data to recipients based outside the European Union or the European Economic Area. The aforementioned data processing entails transfer of data to the servers of Google Inc. in the U.S. We are using the service provider Google, USA, which is certified in accordance to the valid until recently E.U.-U.S. Privacy Shield, however in relation to the transfer of your information and metadata to the U.S. to the aforementioned Service Provider [Google Firebase], where their encrypted storage is taking place in the facilities of the Service Provider following the HTTPS protocol [see <https://firebase.google.com/support/privacy>], taking into consideration the technical and organizational measures for the proper and safe processing of your personal data and the model conventional clauses where Firebase relies on for the transfer of data.

3. How we store and safeguard the information we collect – Data keeping

How long we keep the information the we obtain from you depends on the type of information. The information is kept throughout the period that you are using the Application, as an active user, as well as for the period required by the nature of the information, with the explicit reservation of keeping it for the period specified by the related legislation. In every use, we are doing everything in our power in order for your information to remain safe, by having taken in advance all necessary technical and organizational measures towards that end [firewalls, limited access by the Controller of the Application, Firebase certified according to the main privacy and security standards, see <https://firebase.google.com/support/privacy>].

If it is deemed necessary in order to comply with our legal or regulatory obligations, resolve disputes or strengthen the terms and conditions of use, we can keep some of your data, as required, even if the account has been closed. If a user asks to be deleted by the Controller or is mentioned as abusive by other users, the Controller of EYDAP will keep the electronic address of the user and of the flagged messages for one year, reserving the right to keep the data in case of legal proceedings.

In any event, your personal data is limited to the absolutely necessary for the fulfilment of these purposes, is accurate and is kept for a period of time specified by the purpose of the processing, is protected by adequate security measures and is not transferred to third countries, excluding Firebase as set forth above, but the Controller of the Company solely for the purpose of providing each service.

4. Which are your rights and how to get access to check your information

In any event, you are in control of the processing of your personal data.

You have the option at any time to recall your consent and refer to the instructions for the deletion of your Account: Menu > My Profile > Delete Account.

Data collection through the Application can be terminated with the uninstallation of the Application by the user. The user must follow the procedure indicated by the device, operating system, electronic shop or mobile telephony network.

If you do not wish for your geographical location to be recorded, you are kindly asked to deactivate the Location Services on the settings of your mobile device.

In particular, your rights that are recognized and safeguarded within the applicable legislative framework regarding personal data protection are the following:

- Right to transparent information, communication and modalities for the exercise of your rights (articles 12, 13, 14 GDPR 2016/679), which is your right to be informed about the way your personal data is being used (as done in detail with the present document)
- Right of access (article 15 GDPR 2016/679) to the personal data that we have obtained from you
- Right to rectification (article 16 GDPR 2016/679) of inaccurate personal data that we have gathered for you
- Right to erasure (“right to be forgotten”) (article 17 GDPR 2016/679) of the User account and the information we have obtained concerning you, under the reservations and limitations of each legislation in force and the terms you have accepted regarding the operation of the Application
- Right to restriction of processing your personal data (article 18 GDPR 2016/679), under the conditions of each legislation in force
- Right to object (article 21 GDPR 2016/679) to the processing of your personal data, including the right to object to automated decision-making and profiling, under the reservations and limitations of each legislation in force
- Right to withdraw your already given consent (article 7 GDPR 2016/679), which is your right to withdraw your consent at any time for processing that is taking place based on your consent. The lawfulness of processing your data is not affected by the withdrawal of the consent up to the point that you requested the withdrawal, which means that it does not apply retroactively
- Right of portability, which is the right to receive some of your data in a portable and reusable form.
- You also have the option to appeal to the competent supervisory authority, the Hellenic Data Protection Authority (1-3, Kifissias Avenue, Athens, 115 23, + 30 2106475600, contact@dpa.gr)

You can exercise your rights by filling in the related **Exercise of Rights Form** as displayed via a [hyperlink on the website](#) in the related section of Proper Use and Personal Data Protection Policy, and by sending it via email to the electronic address dpo@eydap.gr or by letter to the address 9, Ilission street, 157 71, Athens. The person in charge to respond, resolve and clarify any of your queries is Ms. Marianna Almpoura , Data Protection Officer (DPO). You are kindly requested to submit your related requests according to the instructions explicitly stated in the Exercise of Rights Form and accompany them with the appropriate proof of personal identification, with the explicit reservation of EYDAP S.A. to ask for additional information to be provided in order to verify and confirm your details.

5. How we transfer the information that we collect internationally

The Company does not transfer your personal data either within the European Union, either outside, to third countries or international organizations, which do not safeguard an adequate level of protection (based on the Adequacy Decision or in compliance with standardized contractual clauses). In relation to data transfer to the service provider Firebase, you have

been informed in detail above. Any transfer follows and complies with the related provisions of the legal framework in force, specifically article 44 GDPR 2016/679. In any event, users will be notified accordingly through an update of the present Policy.

6. How we keep your information safe

In order to protect your privacy, we are applying the optimum practices to safeguard your personal data, via the implementation of the necessary technical and organizational measures as specified in the applicable legislative framework. Data is protected against loss of availability, integrity and confidentiality of the information.

EYDAP S.A. does everything in its power to keep the level of security of the information to the full and complies with the recommended technical measures such as encryption, pseudonymization, anonymization and minimization of data throughout the data processing. Limited access to your data and the information you provide is ensured by an authorized individual of our Company, the Controller of the Application, while the services of Firebase are certified in accordance with the main privacy and security standards (see <https://firebase.google.com/support/privacy>).

7. Response of the Company regarding the personal data of children

Age limit: You must be at least 15 years old to be able to use the services of the Application. In case that the parents of a minor, under age, realize that the Application is being used by the minor without having the right to do so, they are requested to immediately uninstall the Application from the mobile device of the minor. Upon acceptance of the Terms, you declare that you meet the particular age limit or that you have the consent of a parent or legal guardian. In the event that that EYDAP realizes that the Services of the Application are being used by an underage individual without parental consent, it reserves the right to interrupt the provision of the Service and close the account of the user.

8. Notification the Data Protection Officer and exercise of user rights

If you wish to exercise your rights (see Section 4 of the present Policy) or get informed about the processing of your personal data, you are kindly requested to contact EYDAP by sending an email at the address dpo@eydap.gr.

The Data Protection Officer is Marianna Almpoura , who will be in the position to address your queries or requests.

The Company reserves the right, after studying your related request, to proceed within the period of a month or more, in case of a justified delay, to its fulfilment and given that it is legal and sound. Before providing you with personal data, we might ask you for proof of identification and sufficient information regarding your relation with us, through which we can track your personal data.

The Company reserves the right to keep your personal data in those cases that is bound by its legal obligation or exercise of legal claims or fulfilment of its contractual obligations.

9. Update of information about personal data

EYDAP S.A. reserves unilaterally its right to update, modify or revise the present Policy regarding personal data, without prior notice to users aiming at the improvement of its services, its harmonization with the provisions of the existing (national and Community)

legislation regarding the protection of your personal data. For that purpose, you are kindly requested to frequently refer to this Policy in order to get informed about any changes that have taken place.

10. Useful Contact Numbers

A) Details of Controller:

EYDAP S.A.

Address: 156, Oropou street, 111 46 Galatsi, Athens

Telephone: + 30 210 2144444

E-mail: grammateia@eydap.gr

B) Details of Data Protection Officer (DPO):

Marianna Almpoura

E-mail: dpo@eydap.gr

Telephone: + 30 210 7495156 & + 30 210 7495155

C) Details of Hellenic Data Protection Authority:

Headquarters: 1-3, Kifissias Avenue, 115 23, Athens

Call center: +30 210 6475600

Fax: +30 210 6475628

E-mail: contact@dpa.gr