

# AUTHENIX

## Why should you use it?

This service facilitates your app or service to comply with General Data Protection Regulation (GDPR) and provides access to multiple protected citizen science platforms and services via Single-Sign-On.

### 01 REGISTER YOUR APP OR SERVICE ON AUTHENIX.EU



As an app or service provider

### 02 CHOOSE THE INFORMATION YOU NEED FROM YOUR USERS



In the registration process, you can choose what information you want to request from your users (choose none, one or multiple options, or all of them):

- **IdP:** to know from which platform or entity users logged into your app (Facebook, Google, University, etc.)
- **ID:** to create a unique identifier for users
- **Profile:** to collect personal information from users (name, surname, etc.)
- **Email:** to collect the user's email address



If you don't select any options, the user acts de-facto anonymously. If you select Profile or Email, you need to provide a privacy statement, informing users what personal information you are going to collect from them, why and what you are going to do with their data!

### 03 AUTHENIX PROVIDES PERSONAL INFORMATION PER USER



Once you have integrated AUTHENIX, your app or service gets an (OpenID Connect) token including the amount of personal information allowed based on your registration. This way, you don't need to store personal information, which helps you to comply with the European GDPR.



As a user accessing your app or service

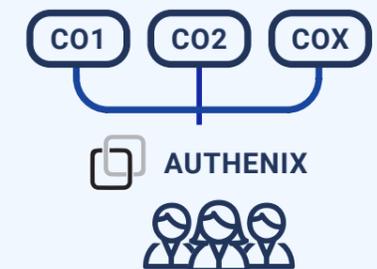
### 04 USERS CAN LOG INTO YOUR APP FROM DIFFERENT PROVIDERS



From now on, anyone accessing your app or service will have multiple provider options to log in, such as Facebook, Google and University (eduGain) accounts.

### 05 USERS WILL HAVE SEAMLESS ACCESS TO ALL THE APPS THAT HAVE INTEGRATED AUTHENIX

This allows users to contribute easily to several citizen science projects hosted on different citizen observatory (CO) apps.



### 06 AUTHENIX ALLOWS END-USERS ...



- To revoke consent for an app to access their personal information
- To be forgotten (all personal data and authorization tokens are deleted)
- To obtain the processing history for their personal information (which app requested personal information and when) as JSON or CSV