Greek Universities Network (GUnet)

Hellenic Academic and Research Institutions

Public Key Infrastructure

Hellenic Academic and Research Institutions Certification Authority (HARICA)

Data Privacy Statement for the

Hellenic Academic and Research Institutions

Certification Authority

Version 1.1

Table of Contents

1 Who we are

Greek Universities Network GUnet ("Controller") is a non-profit organization with members all the Universities and Technological Educational Institutions in Greece and with registered office in the National and Kapodestrian University of Athens – Network Operations Center University Campus that operates and supports the Public Key Infrastructure (PKI) for the Hellenic Academic and Research Institutions. This GUnet service is namely known as the **Hellenic Academic and Research Institutions Certification Authority (HARICA)**.

This Statement concerns the processing of personal data through HARICA and explains the reason for the processing, the way we collect, handle and ensure protection of all personal data provided. It also explains how that information is used and what rights you may exercise in relation to your personal data (the right to access, rectify, block etc.), pursuant to the provisions of the EU General Data Protection Regulation No. 2016/679 ("GDPR").

2 What data (type and categories) is collected?

We collect the data necessary for the provision of the services, such as identifying and contact data ("Personal Data") granted by the subject concerned or by external Reliable Data Sources (e.g. official Government registries, University registries, etc).

Personal Data that MAY be included in digital certificates (depending on the Certificate Type that you choose) can include:

- First Name
- Last Name
- Common Name
- E-mail address
- Locality
- State/Province
- Country
- Job title (professional title) (if relevant)
- Pseudonym (if relevant)
- Company/Organization name (if relevant)
- Organizational Unit name (if relevant)
- Street Address (**Only if explicitly requested by the subject concerned**)
- Government issued ID (Social Security Number, Personal Identification Card, Tax Identification Number, or Passport Number) or other Personal Identifiable Information (**Only if explicitly requested by the subject concerned**).

Personal Data that is not included in digital certificates but that may be requested as part of the Certificate issuance process (e.g. for verifying the identity of an individual). This data can include:

- Home Address
- Telephone number (home/mobile)

- Identification document details (used for identity vetting)

Personal Data is also needed in order to create a user account on our certificate management systems in order to log in to the system and to contact you in case of issues related to the Certificate (expiration, revocation, etc). This Personal Data consists of:

- First Name
- Last Name
- Email
- Phone number(s)
- Username
- Password (chosen by user)

Certain digital certificates, such as device certificates or certificates for electronic seals, do not contain any Personal Data, but Personal Data may be requested as part of the application for such certificates. The name, title, email address and telephone number of the relevant people involved with the certificate request and approval process.

3 Why do we collect your Personal Data? / Legal basis and purposes for the processing

As a Qualified Trust Service Provider, we rely on a variety of information to run our business. In some cases, this information may include data that relates to an identified or identifiable natural person, which is referred to as Personal Data.

The reason that we collect your Personal Data is that we need it for identification and authentication purposes in order to provide you with our products and services, which include the provision of digital certificates and signing services.

In order for you to be informed on all Personal Data that we may ask you to provide for all our different types of Trust Services, please refer to our Certificate Policy and Certification Practice Statement (CP/CPS) at https://repo.harica.gr/documents/CPS.

The legal basis for us processing Personal Data in relation to these services is that processing is necessary for the performance of a contract or to take steps to enter into a contract and for the fulfilment of obligations imposed by national and EU laws and regulations - e.g. Regulation (EU) no. 2014/910 eIDAS, Regulation (EU) 2015/1502 etc.

4 Who is collecting it?

We collect data directly from you, indirectly from reliable data sources (registries) or organizations who have entered into a contract with us (for example to request certificates for their employees/associates/partners/guests).

5 How will it be used?

We use your Personal Data only for the provision of the products and services that we have contracted to provide. This includes:

- Process applications for HARICA products and services
- Provision of technical support
- Issue, revoke and process of digital certificates according to our CP/CPS
- Verification and authentication for the provision of products and services according to our CP/CPS
- Contacting you, as a Subscriber, for issues related to the products and services of HARICA
- Enforcement of legal rights or compliance with legal or regulatory requirements and obligations

6 Who has access to your Personal Data and who will it be shared with?

Access to your Personal Data is provided to authorized staff on a “need to know” basis to deliver the agreed services. Such staff abide by statutory and additional confidentiality agreements. We do not share your personal data with anyone, except to deliver the agreed services. Your information, including Personal Data, will not be sold, exchanged, transferred outside of our organization or given to any other entity for any reason without your prior consent and will not be used for any other than the purposes specified above.

All Personal Data provided for the delivery of the agreed services included in the completed application forms, signed Subscriber Agreements, client contact information and vetting data that supports the issuance of certificates, is retained in HARICA offices for secure storage. This applies also to hard copy physical documents and electronic data.

7 How is your data protected?

We use a combination of technical, administrative, organizational and physical safeguards to protect your personal data. Access to your personal data is restricted to those who are necessary for the delivery of the services. These safeguards are tested as part of our annual audits and certifications. For further details, please see our certifications available at https://www.harica.gr/About/Compliance.

8 Retention Periods

The HARICA CP/CPS in section 5.5.2 (available at https://repo.harica.gr/documents/CPS) requires that audit logs are retained for at least seven (7) years from the date that your digital certificate expires.

We will retain your Personal Data for a period of seven (7) years from the date that your digital certificate expires, unless a longer retention period is required or permitted by law.

As obliged by the eIDAS Regulation for Qualified Trust Service Providers we will retain your Personal Data for a period of seven (7) years from the date that your digital certificate expires.

9 Data Subject Rights

We comply with all relevant Data Protection Laws. These provide a number of rights with regard to your Personal Data.

You have the right to request from us access to and rectification or erasure of your Personal Data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

If you have provided consent for the processing of your Personal Data you have the right (in certain circumstances) to withdraw that consent at any time, which will not affect the lawfulness of the processing before your consent was withdrawn.

You have the right to lodge a complaint with the appropriate Data Protection Authority if you believe that we have not complied with our legal obligations. For further information please visit http://www.dpa.gr.

Please email **personal-data-inquiries AT harica.gr** to make a request under these provisions. In order to help us deal with such request please provide details of the product/service that the request relates to and any other details (such as customer number etc). Please note that we will perform steps to verify your identity before providing any information.

Your requests are subject to our satisfaction regarding the authenticity of the request, and we supply the relevant information within 30 days after validating your request. If for some reason your request is rejected you will be provided with the relevant and detailed explanation.

10 Automated Decision Making and Profiling

An automated decision is defined as a decision which is made following processing of personal data solely by automatic means, where no humans are involved in the decision-making process. We do not use automated decisions in the processing of personal of data.

The GDPR defines profiling as ‘any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements’. We do not perform any profiling.

11 Security

We implement all the appropriate technical, such as security measures (preventative as well as detective) and organizational measures in order to ensure the protection of your Personal Data. We use a variety of security measures, such as encrypted technologies and procedures to help protect your Personal Data from unauthorized access, use or disclosure. The subject is explained in more detail in the administrative, technical and operational controls in sections 5 and 6 of our CP/CPS "Administrative, Technical and Operational controls" and "Technical Security Controls" available at https://repo.harica.gr/documents/CPS. All technical, security and organizational measures are audited on an annual basis by an internationally accredited certification body that provides independent and objective assessments. Conformance Assessment Reports are publicly available at https://www.harica.gr/About/Compliance.

12 Compliance with Data Protection Laws

We fully respect all rights and obligations established and laid out in the Greek and European Legislation regarding protection of personal data and we operate in compliance with:

- All the relevant Data Protection and Privacy Laws, as well as any other regulatory requirement we are subject to
- Any guidance or statutory code of practice issued by Data Protection Authority
- The provisions of our CP/CPS
- Regulation (EU) No 910/2014 eIDAS, Regulation (EU) 2015/1502 and other applicable rules and regulations.

13 Changes to this Data Privacy Statement

This Data Privacy Statement may be modified or updated periodically and without prior notice to you to reflect changes in our personal information practices. You should check our site frequently to see the current Privacy Statement that is in effect.

This Privacy Statement is effective from **May 25th 2018**.

14 Contact

If you have questions regarding this Data Privacy Statement, please contact us via email at **personal-data-inquiries AT harica.gr**.

15 Where to find more details

You can find more details on our public web site (https://www.harica.gr), and more particular the information provided at https://www.harica.gr/About/ where you can find more details about our policies, practices and procedures, along with certifications and Trust Programs that we participate as a Trust Service Provider.