Πανεπιστήμιο Κύπρου
University of Cyprus

Registry .cy

ΣΔΑΠ072

General Data Protection Regulation

Version: 6.0

Issue Date: 20/03/2026

1. INTRODUCTION

This Personal Data Protection Policy governs how the Registry .cy processes the personal data of its customers, ensuring the protection of such information. It applies to all staff employed by the Registry who process or have access to personal data, as well as to customers whose data may be processed.

The Registry .cy is responsible for complying with this Data Protection Policy and adhering to the provisions of the "Law on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (Law 125(I)/2018)" and the provisions of the European Union Regulation "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 - GDPR)."

This policy sets out the terms and conditions under which the Registry .cy collects, processes, and transfers customers' personal data, and aims to inform customers accordingly.

2. LEGAL BASIS

The Registry. cy collects the necessary data as provided by Decree 296/2022, "On the Management and Assignment of the Right to Use Internet Domain Names ending in '.cy' and its Annexes," for the purpose of executing the contract for the assignment of the right to use a domain name. This activity is in accordance with the provisions of the GDPR, specifically Article 6.1(b): "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

Additionally, the Registry .cy collects tax data as required by the "Value Added Tax Law of 2000 (95(I)/2000)" and its subsequent amendments. This activity is in accordance with GDPR Article 6.1(c): "processing is necessary for compliance with a legal obligation to which the controller is subject."

3. DATA COLLECTION

Specifically, the Registry. cy collects the following personal data for each natural person:

- Mandatory fields:

    - Full name
    - Date of birth
    - Identity card or passport number
    - Mobile phone
    - Address
    - Postal code
    - City
    - Email address
    - Password/confirmation password

Data is collected directly from the data subject during the user registration process (account creation) on the Registry's automated system at www.nic.cy. Users can update or modify their personal information through the system. According to Decree 296/2022, Annex I, 11(a): "*The Holder and/or Authorized Representative must update the System with any changes to their details. These details must be up-to-date, accurate, and include, among other things, the correct and complete postal address of the Holder and/or Authorized Representative and/or Administrative Contact.*"

4. DATA PROCESSING

The Registry. cy processes data as follows:

1. Maintains a registry of domain name registrations with domain names and contact links (users). For each user, the personal data listed above is retained.
2. Manages electronic applications submitted by the data subject for the assignment of domain name usage rights via the automated system at www.nic.cy.

The Registry .cy and users' personal data are stored on a server/database hosted on the University of Cyprus's virtual infrastructure. The registry is continuously updated as domain names have renewal periods (1, 2, and 5 years), and if not renewed, they are deleted from the registry.

The Registry .cy reserves the right to send notifications/updates to users' email addresses stored in its database for informational purposes.

5. DATA RETENTION PERIOD

The retention of personal data in the automated System of the Registry .cy will be processed in accordance with the following practices:

- Accounts with users' personal data:

1) Inactive contacts are deleted or anonymized as follows:

   - Technical and Administrative contacts (contact person designated by the licensee) for domain names that become inactive or have been removed as a contact link from a web name will be deleted after one (1) year from their last action in the system.
   - Domain name holders whose usage rights have been deleted are anonymized three (3) years after the domain name is deleted.
   - Financial contacts are anonymized after seven (7) years.
   - Users who created an account but performed no other actions, have not requested a web name, or have been registered as a contact in an online name, are deleted six (6) months after account creation.

2) Draft applications (pending submission) are deleted six (6) months after creation.
3) Electronic requests submitted to the system are handled according to the above timeframes:
   - Request status: rejected – personal data is anonymized.
   - Request status: final approval – personal data of the contact whose domain usage rights have been canceled, deleted, or not renewed is anonymized.

4) The contact's personal data related to domain names whose usage rights have been canceled, deleted, or not renewed is anonymized three (3) years after deactivation.
5) Domain names whose usage rights have been canceled/deleted are deleted three (3) years from the day of deactivation.
6) The personal data of contacts related to domain names for which there is a financial, legal (hierarchical appeal, judicial, or administrative procedure), or other obligation/pending matter are not deleted from the system.
7) Financial data (e.g., invoices, receipts) related to domain names are deleted after seven (7) years, with a possible extension for another seven (7) years if notified by the Tax Authorities.
8) Information contained in legal cases is not deleted. If the case is closed and there are no pending legal issues, the file may be destroyed.

It should be noted that the aforementioned time periods may be extended if justified by objective reasons.

6. DATA SECURITY

The Registry .cy has implemented all necessary technical and organizational measures to ensure data security and protect against unauthorized or unlawful processing, accidental loss, alteration, destruction, or damage, and any other form of unfair processing. These measures ensure a level of security appropriate to the risks associated with processing and the nature of the data.

The Registry .cy has adopted appropriate security procedures in relation to the safekeeping and disclosure of information provided by the subjects themselves. Registry.cy may request proof of identity for identification purposes before proceeding with the disclosure of personal data. Personal data is not used or shared, unless consent or authorization has been given by the subject himself. The processing of personal data is confidential and is carried out exclusively by people under the control of the Data Controller or the Processor, and only on their instructions.

The following technical means are used for the security of personal data:

- Network firewall protection against external attacks and unauthorized access
- Security measures defined by the Registry's security policy
- Registry .cy email security measures
- Access to the automated system only via unique user credentials
- Certified software and hardware are used to ensure the quality and security of the transmitted information,
- Daily backup copies of the database

7. DATA TRANSFER TO THIRD PARTIES

According to the agreement for the registration of a domain name ending in .cy, and its terms and conditions, personal data provided during the registration of a domain name may be transferred in accordance with the provisions of the Personal Data Processing Law in the following cases:

- To government agencies or law enforcement authorities of the Republic of Cyprus (competent state authorities), such as judicial authorities and the Cybercrime Service, for purposes related to the security or defense needs of the Republic of Cyprus.
- To third parties only if requested by a court order. Exceptionally, customer data is transferred after notification and consent.

- To countries inside and outside the European Union
- To the Office of the Commissioner for Electronic Communications and Postal Regulation (OCECPR) and the Registry's Legal Advisor in cases of complaints, illegal activity, or dispute resolution
- To ICANN (Internet Corporation for Assigned Names and Numbers) or WIPO (World Intellectual Property Organization) for complaint management and dispute resolution

8. SCOPE

This policy applies to all personal data processed by the Registry .cy on behalf of its customers and processed in the context of the Registry's purposes and services. Personal data may be in electronic or paper form.

9. RIGHTS OF DATA SUBJECTS

The GDPR aims to strengthen the fundamental rights and freedoms of natural persons, especially the protection of personal data and its free movement. Accordingly, the General Data Protection Regulation (GDPR) recognizes the following rights for data subjects:

1. **Right to be Informed:** Data subjects have the right to be informed about the processing of their personal data, the reasons for collection and processing, by whom, and with whom their data is shared.
2. **Right of Access:** Data subjects can request and receive a copy of any information held about them.
3. **Right to Rectification:** Data subjects can request correction of inaccuracies or completion of incomplete data.
4. **Right to Erasure (Right to be Forgotten):** Data subjects can request the deletion of their personal data when they no longer wish it to be processed or retained, provided that the data is not required for a specific lawful purpose.
5. **Right to Restriction of Processing:** Data subjects can request the restriction of processing when the accuracy of the data is disputed, when processing is unlawful, when the controller no longer needs the personal data for the purposes of processing, or when the controller intends to erase the data.
6. **Right to Data Portability:** Data subjects can receive their personal data for private use and transfer it from one controller (e.g., Registry.cy) to another controller “without objection”. They can also request that the controller (Registry.cy) provide

their data in a commonly used format or directly transfer it to another controller, if technically feasible.

7. **Right to Object:** Data subjects can object at any time, for reasons related to their particular situation, to the processing of their personal data. They can also object to processing for direct marketing purposes, including profiling.
8. **Rights related to automated decision-making, including profiling:** Data subjects can object to decisions made by automated means.

Data subjects have the right to access their personal data (in accordance with the "Right of Access" referred to above) by submitting the relevant request, titled **"Request for Access to Personal Data", either electronically to the email address domains@nic.cy or by mail to: Registry .cy, P.O. Box 20537, 1678 Nicosia, CYPRUS.**

Requests are archived for two years after fulfillment and then deleted.

The Registry .cy is committed to responding to your request within thirty (30) days from the date of submission. However, in cases where fulfilling your request is not possible for the Organization, we will provide a reasoned explanation for the inability to comply, along with the expected date of response, which will not exceed ninety (90) days from the original submission of your request.

Please be informed that you have the right to contact the Office of the Commissioner for Personal Data Protection regarding any issues related to the processing of your personal data. For information on the Commissioner's authority and the procedure for filing a complaint, you can visit: http://www.dataprotection.gov.cy/.

10. OBLIGATIONS

To comply with the Regulation, personal data must be collected and processed in a transparent manner with respect to the data subject, must be secured, and must not be transferred unlawfully to third parties. All personnel employed by the Registry.cy who process and/or have access to personal data comply with the following principles established by the General Data Protection Regulation:

10.1 GDPR PRINCIPLES

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner with respect to the data subject. Processing is considered lawful when:
    - Consent has been given by the data subject,
    - It is necessary for the performance of a contract,

        - Compliance with a legal obligation of the Data Controller (Registry .cy) is required,
        - It is necessary to protect the vital interests of the data subject,
        - It is necessary for the performance of a task carried out in the public interest,
        - It is necessary for the legitimate interests of the Data Controller (Registry .cy).
- **Purpose Limitation:** Personal data should be collected for a specific purpose or for several specified purposes and must not be further processed in a way that is incompatible with those purposes. Personal data must not be used or shared for any other purpose unless the data subject has given explicit consent.
- **Data Minimization:** Data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.
- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date or corrected.
- **Storage Limitation:** Personal data must not be stored or retained for longer than is necessary for the purposes for which they are processed.
- **Integrity and Confidentiality:** Appropriate technical and organizational measures must be taken to ensure the security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using suitable technology.
- **Accountability:** The principle of accountability is a cornerstone of the General Data Protection Regulation (GDPR). Under the GDPR, businesses and organizations must comply with all data protection principles and be able to demonstrate their compliance.

10.2 INFORMATION TO DATA SUBJECTS AND LAWFUL PROCESSING

Data subjects must be informed about the protection of their personal data and their rights before data is collected or processed.

10.3 PROCESSING OF PERSONAL DATA BY THIRD PARTIES

Sufficient assurances from third parties that processing complies with the Regulation:
When processing is to be carried out on behalf of the Registry .cy by third parties (processors), the Registry uses only processors who provide sufficient assurances regarding the implementation of appropriate technical and organizational measures, so that the processing meets the requirements of the Regulation and ensures the protection of the data subject’s rights.

No engagement of another processor without the Registry's approval: A processor must not engage another processor without prior specific or general written authorization from the Data Controller. In the case of general written authorization, the processor must inform the Data Controller of any intended changes concerning the addition or replacement of other processors, thereby providing the Data Controller the opportunity to object to these changes.

Processing by the processor is governed by a contract:
Processing carried out by the processor is governed by a contract or other legal act under Union law or the law of a Member State, which binds the processor to the Data Controller and specifies the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects involved, as well as the obligations and rights of the Data Controller.

10.4 DATA PROTECTION BY DESIGN AND BY DEFAULT

Appropriate technical and organisational measures at the time of determining and during processing: Taking into account the risks of varying likelihood and severity to the rights and freedoms of natural persons resulting from processing, effective technical and organizational measures must be implemented both at the time of determining the processing means and during the processing itself. Such measures, including pseudonymization, should be designed to apply data protection principles, such as data minimization, and to integrate the necessary safeguards into the processing so that the requirements of the Regulation are met and the rights of data subjects are protected.

Processing only the personal data necessary for each specific purpose:
Appropriate technical and organizational measures must be applied to ensure that, by default, only personal data that are necessary for the specific purpose of the processing are processed. This obligation applies to the scope of personal data collected, the degree of their processing, the storage period, and their accessibility. In particular, these measures ensure that, by default, personal data cannot be accessed by an indefinite number of individuals without the intervention of the data subject.

10.5 PERSONAL DATA BREACH

It is the responsibility of all personnel employed by the Registry .cy to immediately notify the authorized Data Controller in the event that personal data is accidentally or unlawfully destroyed, lost, altered, disclosed, accessed, stored, or otherwise processed in a manner not in accordance with the prescribed regulations, policies, or procedures of the Registry.

In the event of a personal data breach, the Registry, through the Data Security Officer, shall notify the supervisory authority (Office of the Commissioner for Personal Data Protection) within 72 hours of becoming aware of the incident, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Any

unlawful or non-compliant processing of personal data may result in disciplinary action and could lead to criminal prosecution.

11. DATA PROTECTION OFFICER

The Data Protection Officer is responsible for monitoring compliance with the Regulation within the Registry .cy. The role is advisory. Primary duties include informing the Data Controller of their obligations and providing guidance upon request. The DPO also serves as the point of contact between the Organization and the Office of the Commissioner for Personal Data Protection.

Within the scope of monitoring compliance, the Data Protection Officer may:

- Collect information to identify processing activities,
- Analyze and audit the compliance of processing activities, and
- Inform and/or advise the Data Controller or the processor on matters concerning compliance with the Regulation.

12. DEFINITIONS

“Personal data”: any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one whose identity can be determined, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

“Processing”: any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

“Profiling”: 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 work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements of that natural person.

“Pseudonymization”: the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical

and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person.

“Data Controller”: the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its appointment may be provided by Union or Member State law.

“Processor”: a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

“Third party”: any natural or legal person, public authority, agency, or body other than the data subject, the controller, the processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

“Consent” of the data subject: any freely given, specific, informed, and unambiguous indication of the data subject’s wishes, by statement or clear affirmative action, signifying agreement to the processing of personal data relating to them.

“Personal data breach”: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

“Supervisory authority”: an independent public authority established by a Member State (Commissioner for the Protection of Personal Data).