University of Cyprus

.cy

Registry .cy

Personal Data Privacy Policy

Edition: 5

Publication Date: November 2023

1. INTRODUCTION

The Personal Data Privacy Policy governs the way in which the .cy Registry processes its customers' personal data in order to ensure the protection of their personal data. It is addressed to all employees that work at the .cy Registry who process and/or have access to personal data, as well as to the Registry's customers whose data we may process.

It is the responsibility of the Registry to comply with this Data Protection Policy and to comply with its provisions "on the Protection of Natural Persons Against the Processing of Personal Data and for the Free Movement of such Data -Law of 2018 (Law 125 (I)/ 2018)" as well as the provisions of the act of the European Union entitled "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 for the free movement of such data and for the repeal of Directive 95/46/EC (General Data Protection Regulation)".

This policy sets out the terms and conditions under which the .cy Registry executes the collection, processing, and transfer of its customers' personal data and informs them accordingly.

2. LEGAL BASIS

The .cy Registry collects the necessary data that are provided in accordance with the Decree R.A.A. 296/2022, "On the Definition of the Management and Granting of License for Domain Names" with ".cy" suffix and its Annexes, for the purpose of executing the contract for the granting of a license for the domain name's use. This activity is in accordance with the provisions of the General Data Protection Regulation and in particular Section 6.1 (b): "processing is necessary for the performance of a contract of which the data subject is a contracting party or to take measures at the request of the data subject before the conclusion of the contract".

In addition, the .cy Registry collects the necessary tax data that are required in accordance with the "Value Added Tax Law 2000 (Law 95 (I) / 2000)" and its subsequent amendments. This activity is in accordance with the provisions of the General Data Protection Regulation and specifically with Section 6.1 (c): "processing is necessary for compliance with the legal obligation of the data controller".

3. DATA COLLECTION

Specifically, the .cy Registry collects the following personal data for every natural or legal person:

Compulsory fields:
Natural persons:

- Full name
- Date of birth
- ID or passport number

Legal entities:

- Company name
- Company registration number

- Address
- Postcode
- City
- Country
- Email address
- Access code/code confirmation

The collection of the above personal data is performed by the subject himself/herself through the process of user registration (account creation) in the automated System on the website www.nic.cy of the Registry. The user can verify/update his/her personal information through the automated System. In accordance with Decree R.A.A. 296/2022, Annex I, 11(a), *The Registrant and/or the Authorised Representative are required to inform the System of any changes to their details. These details need to be up-to date, accurate and include, among other things, the correct and complete postal address of the Registrant and/or the Authorised Representative and/or Administrative Contact.*

4. DATA PROCESSING

The .cy Registry processes data as follows:

1. It maintains a Registry with the domain names and contacts (users). The aforementioned personal data are kept for every user.

2. It manages the online application that is submitted electronically by the subject for the granting of a license to use a domain name through the automated System on the website www.nic.cy of the Registry.

The Registry of domain names and the personal data of the users are kept in a server - database of the automated System that is hosted in the virtual infrastructure of the UCY. The Registry is updated on a

constant basis as the domain names have renewal periods (1, 2 and 5 years) and in case of non-renewal they are erased from the Registry.

The .cy Registry has the right to send announcements/updates to user's email accounts maintained in its database for information purposes.

4.1 CALL RECORDING

For security and quality improvement purposes all calls are recorded so that there is availability and direct access to data and information, when needed. Specifically, for internal administrative operations such as customer service and provision of operational support, clients' personal data collected by Registry .cy via the call center, might be necessary to be accessed and processed.

It is clarified though that for each call, the recording involves only the conversation between the data subject and the call center (this includes the voice and any other data given by the data subject during the call, such as name, phone number and email). This data is stored on the University of Cyprus infrastructure for a period of fifteen (15) days only.

Data subjects calling the Registry .cy are basically giving their consent for processing their personal data as described above.

5. PERSONAL DATA RETENTION PERIOD

The retention of personal data in the automated Registry System will be processed in accordance with the practices as follows:

1. Accounts with the users' personal data will be processed as follows:
    1. Inactive contact will be deleted or be anonymized according with the below:
        - Technical and Administrative contact who registered in a domain name that has become inactive or has been removed as a contact from the domain name will be deleted after the end of one (1) year that the specific contact has not performed any action in the System
        - The Registrant contact will be anonymized when three (3) years have passed from the deletion of domain name.
        - The Billing contact will be anonymized in seven (7) years.
        - A user account that has been created but has not performed any other action, nor requested domain name, nor registered as a contact on any domain name, will be deleted six (6) months from the account's creation date.

2. Applications in a draft form will be erased after the end of 6 months from their submission date to the System.

3. The online (electronic) requests that have been submitted to the System will be handled according with the above time intervals as follows:

    a. Request status: rejection – The contact's personal data will turn anonymized.

b. Request status: final approval –The personal data of a contact who had a domain name license and the license has been canceled, deleted or not renewed will turn anonymized.

4. A contact's personal data that are related to a domain name whose license has been canceled, deleted or not renewed will turn anonymized when three (3) years have passed from the day of its deactivation.

5. Domain names whose license has been canceled/deleted will be deleted from the System when three (3) years have passed from the day of their deactivation.

6. A contact's personal data that are related to a domain name for which there is a financial, legal (hierarchical appeal, court, administrative procedure) or other obligation/pending matter are not deleted from the System.

7. Financial data (e.g. invoices, receipts) related to the domain names will be erased in seven (7) years with an extension of another seven (7) years in case of notification by the Tax Services.

8. The information included in legal cases is not deleted. If the case is completed and there are no outstanding legal issues then the file may be destroyed.

The above time frames may be extended in case it is required by objective reasons.

6. DATA SECURITY

The .cy Registry has taken all necessary technical and organizational measures to secure/protect the data from unauthorized or illegal processing, accidental loss, alteration, destruction or damage and from any other form of improper processing. These measures ensure a level of security that corresponds to the risks involved in processing and the nature of the data processed by the Registry.

The Registry has adopted the appropriate security procedures in relation to the safekeeping and disclosure of information that is provided by the subjects themselves. The Registry may request proof of identity before proceeding with the disclosure of personal data. Personal data are not used or shared unless the relevant consent or authorization has been given by the subjects themselves. The processing of personal data is confidential. It is carried out exclusively and solely by persons under the control of the controller or the processor and only under his/her instructions.

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

o Firewall (network firewall, unauthorized access)

o Security measures determined by the security policy of the University of Cyprus

o Security measures of the e-mail of the University of Cyprus

o Access to the automated Registry System is possible only through a unique user password and access password

o Software and/or hardware that has been certified for its quality is being used, and which ensures the security of the transferred information

o Database backups on a daily basis

7. DATA TRANSFER TO THIRD PARTIES

Under the registration agreement for the .cy domain names, terms and conditions, with the domain name registration, personal data may be transferred in accordance to the provisions of the Personal Data Processing Law in the following cases:

- To Government bodies or Law enforcement agencies (competent authorities of the Republic of Cyprus) such as Judicial authorities, Cybercrime Service of Cyprus Police, for the purposes of the security or defence needs of the Republic of Cyprus.
- To Third parties only if requested by a Court Decree. Exceptionally, a customer's personal data are transferred after s/he been informed and we have his/her consent.
- In Countries inside and outside the European Union.
- To the OCECPR and the Legal Consultant of the Registry, in cases concerning a complaint, illegal activity or dispute resolution procedure.
- To the ICANN (Internet Cooperation for Assigned Names and Numbers) or the WIPO for complaint management and dispute resolution procedure.

8. SCOPE

This policy applies to all personal data that are processed by the .cy Registry on behalf of its customers and are processed for achieving the purposes and services of the Registry. Personal data may be in electronic or printed form.

9. RIGHTS

The Regulation aims to strengthen the fundamental rights and freedoms of natural persons, in particular the protection of personal data and their free movement. Therefore, the General Data Protection Regulation recognizes certain rights of the personal data subjects as follows:

9.1 Right to be informed: Data subjects have the right to be informed about the processing of their personal data, the reasons why they are collected, processed and by whom, and with whom they share their personal data.

9.2 Right to access: Data subjects have the right to request and receive a copy of any information held about them.

9.3 Right to rectification: Data subjects have the right to request rectification of any inaccuracies or incorrect information as well as to complete incomplete data about them.

9.4 Right to erase (to be forgotten): Data subjects, when they no longer wish the process and maintaining of their personal data, can request their erasure, provided that the data are not kept for a specific legal and declared purpose.

9.5 Right to restrict processing: Data subjects have the right to ask the controller to restrict processing when the accuracy of the data is disputed or is illegal or the controller no longer requires the personal data for processing purposes, or when the controller is about to erase them.

9.6 Right to data portability: Data subjects have the right to receive personal data for further private use as well as to transfer them from one controller (University of Cyprus) to another "without objection". They can also ask the controller (University of Cyprus) to receive their data in a widely used and machine-readable format, as well as to transfer the data directly to another controller, if this is technically feasible.

9.7 Right to object: Data subjects have the right to object, at any time for reasons related to their particular situation, the processing of personal data. In addition, when personal data are processed for the purposes of direct marketing (including profiling), data subjects have the right to object to such processing.

9.8 Right to objection: Data subjects have the right to object to decision-making by automated means.

Data subjects can have access to their personal data (in accordance with the "Right to Access" as aforementioned) by submitting the relevant request "Request to Access Personal Data" electronically at the email address domains@nic.cy or by post at the .CY Name Registry, PO Box 20537, 1678 Nicosia, CYPRUS.

The specific requests will be archived for a period of 2 years after their completion and will then be deleted.

The .cy Registry undertakes to respond to your request within thirty (30) days from the date of submission. However, in cases where meeting your request is impossible for the Organization, we will inform you of the reasons for this rejection, as well as the estimated date of response to your request, which will not exceed a total of ninety (90) days from the initial submission of your request.

We inform you that you have the right to apply to the Office of the Commissioner for Personal Data Protection for issues related to the processing of your personal data. For the responsibilities of the relevant Office and for how to submit a complaint, you can visit the website http://www.dataprotection.gov.cy/

10. LIABILITIES

In order to comply with the Regulation, personal data must be collected and processed in a transparent manner in relation to the data subject, to be secured and not to be illegally transferred to third parties. All employees that work at the .cy Registry who either process and/or have access to personal data must comply with the following principles as set out in the General Data Protection Regulation:

10.1 PERSONAL DATA PROTECTION PRINCIPLES

10.1.1 Legality, Objectivity and Transparency: Personal data must be processed in a fair, legal and transparent manner in relation to the data subject.

Legal processing exists when:

o Consent has been given by the data subject

o It is done in the context of contract execution

o Compliance with the legal obligation of the Controller (University of Cyprus) is required

o It is necessary to safeguard the vital interests of the data subject

o It is part of fulfilling a duty in the public interest

o It is part of the legal interest of the Controller (University of Cyprus)

10.1.2 Purpose Limitation: Personal data should be only obtained for a specific purpose or for more specific purposes and should not be further processed in any way that is incompatible with this purpose or purposes. Personal data must not be used or shared for any other purpose unless the relevant consent has been given by the data subject.

10.1.3 Data Minimization: Personal data must be relevant to the purpose but no more than what is required for the intended purpose that they are being processed for.

10.1.4 Data Accuracy: Personal data must be accurate and updated/rectified when required.

10.1.5 Limited Data Retention: Personal data should not be stored/retained for longer than required.

10.1.6 Integrity and Confidentiality: The appropriate technical and organizational guarantees must be obtained in order to ensure the protection of personal data, including protection against unauthorized or illegal processing and from accidental loss, destruction or damage, using the appropriate technology.

10.1.7 Accountability: The principle of accountability is a cornerstone of the General Data Protection Regulation (GDPR). According to the GDPR, businesses and organizations are responsible for complying with all data protection principles as well as to demonstrate such compliance. In addition, personal data must not be transferred outside the European Union. If it is necessary to transfer personal data outside the European Union, the advice of the Data Protection Officer must be sought.

10.2 INFORMING THE DATA SUBJECTS AND LEGAL PROCESSING

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

10.3 PERSONAL DATA PROCESSING BY THIRD PARTIES

10.3.1 Adequate assurances from third parties that the processing meets the requirements of the Rules: When processing is to be performed on behalf of the .cy Registry by third parties (processors), the Registry shall only use processors that provide sufficient assurances of the implementation of appropriate technical and organizational measures, so that the processing meets the requirements of the Regulation and the protection of the data subject's rights is ensured.

10.3.2 Non-recruitment of another processor without the approval of the Registry: The processor shall not hire another processor without the prior specific or general written authorization of the controller. In case of a general written authorization, the processor shall inform the controller about any intended changes concerning the addition or replacement of the other processors, thereby allowing the controller to object to such changes.

10.3.3 The processing by the processor is governed by a contract: The processing by the processor is governed by a contract or another legal act governed by a contract or another legal act by the Union or a Member State law, which binds the processor in relation to the controller and determines the object and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller.

10.4 DATA PROTECTION BY DESIGN AND BY DEFINITION

10.4.1 The appropriate technical and organizational measures at the time of the determinination of the means of processing and at the time of the processing itself: Taking into account the risks of varying likelihood and severity for rights and freedoms of natural persons by the processing, both at the time of the determination of the means of processing and at the time of the processing itself, the appropriate technical and organizational measures shall be implemented, such as pseudonymization, which are designed to implement data protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation and protect the rights of data subjects.

10.4.2 The processing of only necessary personal data solely for the purpose of processing: Appropriate technical and organizational measures must be implemented in order to ensure that, by definition, only personal data which are necessary for the purpose of processing are being processed. This obligation applies to the extent of the collected personal data, the degree of processing, the storage period and their accessibility. In particular, these measures shall ensure that, by definition, personal data are not made accessible without the intervention of the natural person to an indefinite number of natural persons.

10.5 PERSONAL DATA BREACH

It is the responsibility of all employees that work at the Registry to notify immediately the authorized controller in the event that either accidentally or unlawfully personal data are destroyed, lost, altered, disclosed or otherwise accessed, stored or otherwise processed in a manner that does not comply with the framework of the legal regulations, policies or procedures of the Registry.

In the event of personal data breach, the Registry shall, through the data protection officer, notify the supervisory authority within 72 hours of becoming aware of the personal data breach (Commissioner for Personal Data Protection), unless it is unlikely that the personal data breach endangers the rights and freedoms of the natural persons. Any illegal or unlawful processing of personal data will result in disciplinary action which may also lead to criminal prosecution.

11. DATA PROTECTION OFFICER

The Data Protection Officer is responsible for monitoring the compliance with the Regulation within the University. His/her role is advisory. His/her main duties are to inform the controller about his/her obligations, to give advice, if requested. S/he is also the contact link between the Organization and the Office of the Personal Data Protection Commissioner.

In the context of his/her duties with regard to the monitoring of compliance, the Data Protection Officer may:

• collect information in order to identify processing activities,

• analyze and monitor the compliance of processing activities, and

• inform and/or advise the controller or processor on issues related to the compliance with the Regulation.

The contact details of the person in charge of Personal Data Protection (PDP) of the University of Cyprus are the following:

Chryso Agapiou

Accountant 1st

Data Protection Officer (DPO)

Rector's Office - University of Cyprus

Phone: +357 22894361

Email: dpo@ucy.ac.cy

12. DEFINITIONS

12.1 "personal data" means any information relating to an identified or identifiable natural person ("data subject"); the identifiable natural person is that whose identity can be verified, directly or indirectly, in particular by reference to an identifier, such as a name, identity number, location data,

online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

12.2 “processing” means any operation or set of operations which is 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, information search, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

12.3 “profiling” means 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

12.4 “pseudonymization” means 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 they cannot be attributed to an identified or identifiable natural person

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

12.6 “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

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

12.8 “consent” of the data subject: any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which s/he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

12.9 “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

12.10 “supervisory authority” means an independent public authority which is established by a Member State (Commissioner for Personal Data Protection)