

Re-identification Challenge

Terms & Conditions for participants

Version: 3.7

Date: 30/08/2024

Please kindly review the document thoroughly, sign it digitally and send it to reid_challenge@iislafe.es. In case of any questions or problems, do not hesitate to contact reid_challenge@iislafe.es .

1. The Challenge

- 1.1. AI4HI (AI for Health Imaging) is a network of European research organizations and companies that are working together to develop and deploy artificial intelligence (AI) technologies for health imaging. The network was launched in 2019 with funding from the European Union's Horizon 2020 research and innovation program.
- 1.2. HULAFE (referred to as the “**Organizer**” or “**Controller**”) is organizing the Challenge.
- 1.3. HULAFE is organizing this Challenge (the “**Challenge**”) to validate the robustness of 2 de-identification methods used in AI4HI projects. Participants will show their skills to re-identify patients by the metadata of the DICOM images.
- 1.4. The Challenge will take place from July 2024 up until the end of September 2024.
- 1.5. The Data will be available through the Intercambio Service, hosted at the UPV (Polytechnic University of Valencia) (the “**Platform**”).
- 1.6. All the details related to the Challenge are included in this “Terms and Conditions” document together the “Re-identification Challenge Description” document.

2. Eligibility

- 2.1 The Challenge is open to researchers from any of the four ongoing projects in AI4HI network (EuCanImage, INCISIVE, ProCacer-I and ChAImeleon) and EUCAIM and prior acceptance by the Organizer, which will be notified after completing and submitting the registration form created for such purpose.
- 2.2 Participation in the Challenge constitutes the Participant's full and unconditional agreement to and acceptance of these terms and conditions, otherwise referred to as rules of the Challenge (“**Terms**”). The term “you” refers to you, the “**Participant**”.
- 2.3 Participants will be restricted to ongoing projects of AI4HI and EUCAIM researchers.

3. Application

- 3.1 Applications will be accepted from the announcement in April 2024 until the end of the Challenge (the “**Application Period**”).
- 3.2 Each Participant must complete the registration form. Moreover, they must send this Terms and Conditions document digitally signed and duly fulfilled with all information requested to reid_challenge@iislafe.es
- 3.3 After careful assessment, the Organizer will notify the selected Participants of their acceptance to participate in the Challenge and will send more information to them.
- 3.4 Participants should register with their real names, affiliation (including the full name of the university/institute/company) and affiliation e-mails. To qualify for ranking on the leaderboard, true names and affiliations must be displayed.
- 3.5 Each Participant can only be a member of a single team.

- 3.6 Any individual participating with multiple or duplicate profiles will be disqualified.
- 3.7 The Organizer reserves the right to verify the eligibility of Participants and check their identities and reserves the right of admission based on its sole discretion.
- 3.8 Participants shall follow relevant institutional policies and applicable European and national laws and regulations (if any) concerning the completion of ethics review or approval that may be required for participation in the Challenge. When applicable due to their own circumstances, Participants shall submit an ethical approval validly issued by a duly accredited Ethics Committee, DPIA and/or an ethical (AI) impact assessment (e.g. ALTAI methodology).

4. Participation

- 4.1 The Challenge will run from the beginning of July 2024 until the end of September 2024. Participants will be able to download a controlled data set of medical studies. Participants will use their own resources to achieve the objective of the Challenge.
- 4.2 Participants acknowledge and accept that acceptance of the terms and conditions of the Platform shall be required in order to participate in the Challenge.
- 4.3 The Organizer will not reimburse any expenses or costs for Participants.

5. Data

- 5.1 Participants will have access to the Platform where the corresponding DICOM imaging studies will be shared (accessible through a single-access link) with the Participants (the “Data”).
- 5.2 Data always remains the sole property of the Organizer and Participants acknowledge and accept that they will not acquire any intellectual property right or any other right over the Data, other than as set forth herein.
- 5.3 The Organizer grants the Participants a royalty-free, non-sublicensable, non-transferable, non-commercial, non-exclusive, revocable license to use the Data for the Challenge.
- 5.4 Participants expressly agree to exclusively use the provided Data for participation in the Challenge and not to distribute, transfer, share or disclose it in any way or form.
- 5.5 After the Challenge (or any time before upon request by the Organizer), the Participants must destroy all Data disclosed by the Organizer in their possession, stored electronically and/or on record-bearing media as well as any copies thereof. Upon request by the Organizer, Participants shall confirm in writing within (14) fourteen days such destruction of the Data and any copies thereof.
- 5.6 Participants will not assist any third party in reverse engineer, decompile or disassemble the Data.
- 5.7 Participants will not, either alone or in concert with any other information, make any effort to contact individuals who are or may be the source of the information in the Data.
- 5.8 Participants expressly agree not to make more than one account for accessing and/or downloading the Data and submitting their entries (“**Submissions**”).

6. Intellectual Property

- 6.1 Participants warrant that their Submissions are their original work and, as such, they are the sole and exclusive owners and rights holders of their respective Submissions. Participants shall have the right to make the Submission and grant all required licenses.
- 6.2 Participants agree not to make any Submission that infringes any third-party proprietary rights, intellectual property rights, industrial property rights, personal or moral rights, or any other rights, including, without limitation, copyright, patent, trade secret, privacy or confidentiality obligations.
- 6.3 The ownership of any intellectual property developed by the Participants during and within the scope of the Challenge will remain with the Participants.

- 6.4 The Participants shall not acquire any full or partial intellectual property right (or any other rights of any kind) over the Challenge or the Platform, nor on any names or trademarks associated with them, used alone, in association with or as part of another word or name.

7. Personal Data

- 7.1 The Organizer may collect personal data (understood as information that relates to an identified or identifiable individual) from the Participants in the application process and throughout the Challenge. This personal data will only be used for communication by the Organizer with the Participants relating to the Challenge and any Challenge-related information, such as the distribution of the Prizes.
- 7.2 Explicit consent for any other uses of Participants' personal data will be requested if needed.
- 7.3 By entering the Challenge, Participants agree to give the Organizer access to the information they provide. This includes information you provide by your participation in the Challenge, forums or message boards, the information you provide to us if you contact us (for example, to report a problem or raise a query or comment), and details of the resources accessed.
- 7.4 In accordance with GDPR, Participants may exercise their rights of access, rectification, erasure, restriction of processing, objection, and portability by contacting the Organizer via the Email Organizers section.
- 7.5 Participants will not use the Data, either alone or in concert with any other information, to make any effort to contact individuals who are or may be the source of the information in the Data.
- 7.6 Privacy Policies of the Platform apply. You can find more information about how your personal data are processed in Annex II.

8. Confidentiality

- 8.1 All Confidential Information disclosed by the Organizer to Participants in connection with the Challenge:
- shall be used by Participants exclusively for participation in the Challenge;
 - must not be distributed or disclosed in any way or form by Participants;
 - must be kept confidential by Participants; and
 - remains the sole property of the Organizer.
- 8.2 "**Confidential Information**" means any information and data, including, but not limited to, the Data, any kind of business, commercial, code, dataset or technical information, and data disclosed in connection with the Challenge irrespective of the medium in which such information or data is embedded.
- 8.3 A patient will be considered to be re-identified when the Participants provide one of the following personal data according to their hospital records that provided the medical studies for this Challenge:
- Name and surnames.
 - ID Number (passport number, DNI, Codice Fiscale, Número de Identificação Fiscal).
 - Phone number.
 - Full postal address.
 - E-mail address.
- 8.4 In case of re-identification of patient Data, you are allowed to keep the identified information until the end of the challenge, however, you are not allowed to use it for anything other than sharing the results in the appropriate format with the Organizer.
- 8.5 The results of the Challenge will consist of a template completed with the identified personal information of the medical studies and a written document detailing the undertaken

process. Even if patients have not been able to re-identify the images, they should upload a document with the process they have followed to try to do so.

- 8.6 After the Challenge (or any time before upon request by the Organizer), the Participants must destroy all Confidential Information disclosed by the Organizer in their possession, including Confidential Information stored electronically and/or on record-bearing media as well as any copies thereof.
- 8.7 The Participant shall have the status of Data Processor if the purpose of the request for re-identification of personal data is met and/or if the images are downloaded in his/her/its own premises. By virtue of this, the individual participant, or the entity in which he or she provides his or her services, shall assume the following contractual obligations. As processor he/she/it shall:
- a. process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - b. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - c. accept, apply, and take all measures of security required pursuant to Article 32 of GDPR. These measures should be expressly accepted by each member of the team when they first join the platform;
 - d. not subcontract any other third party as sub-processor;
 - e. assist the controller in ensuring compliance with the obligations pursuant to Articles 32 of GDPR in case of security incident or data breach;
 - f. make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this paragraph and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
 - g. Subcontracting of processing environments is only allowed if
 - i. The data processing will be carried out after the download of the images on the participant entity's own resources.
 - ii. Under the conditions provided for in Article 28 of the GDPR, the participating entity uses processing resources provided by a third party with which there is a processor contract.
 - iii. Except in the cases and with the guarantees of the RGPD, there is no international transfer of data.
 - iv. A copy of the contract with the subcontractor will be provided to the organiser of the challenge or a certificate from its data protection officer.
 - v. At the end of the challenge the data will be deleted by a secure deletion which must be certified by the challenger.

8.8 Access to the data is not allowed from a third country other than the European Economic Area.

9. Representations & Warranties

- 9.1. Participants represent and warrant that:
- (i) The posting of your content (the **“Content”**) within the scope of your participation in the Challenge (including the information you provide by your participation in the Challenge in forums or message boards) does not violate the privacy rights, publicity rights, copyrights, contract rights, or any other rights of any person.
 - (ii) The Content will not cause the Organizer to breach any law, regulation, code, or other legal obligation and will not or could not be reasonably considered defamatory, disparaging, seditious, offensive, threatening, abusive, in breach of confidence or breach of privacy.
 - (iii) The Content does not contain software viruses, or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment.
- 9.2 The Organizer reserves the right to modify or remove any Content at any time.

10. Verification of Submissions

- 10.1. After the Challenge has finished, the final rank will showcase the top 4 Participants (**“Winners”**), and the Winners will be notified using the institutional email indicated in the registration form.
- 10.2. Participants agree that the decision on the Winners shall be final and binding for all Participants and shall not be subject to dispute in a court of law. Participants shall have no right to a justification of the decisions made by the Organizer.
- 10.3. The award of the Prizes may be subject to verification of the identity, qualifications, and role of the Participant in the creation of the Submission.
- 10.4. The Organizer may deem a Participant ineligible to win if the Organizer reasonably believes that the Participant has attempted to undermine the legitimate operation of the Challenge by cheating, deception, or other unfair or dishonest practices.
- 10.5. In the event of a disqualification, the Organizer may award the applicable Prize to an alternate Participant.
- 10.6. The Organizer is not responsible for Submissions not received due to lost, failed, delayed or interrupted connections or miscommunications or other electronic malfunctions.

11. Monetary Prizes & Validation

- 11.1. After the Challenge has finished, the top 4 Participants will be notified by email, and the Final Rank of the winning Participants (the **“Winners”**) will be announced in October 2024.
- 11.2. Monetary prizes will be payable to the Winners (the **“Prizes”**) as follows:

Final Rank	Prize
1st place:	5,000 €
2nd place:	3,000 €
3rd place:	1,000 €
4th place:	1,000 €

- 11.3. The Prizes will be sent wired to the Winners' bank accounts only after receipt by the Organizer of the required information or documentation (if any) for the delivery of the Prizes. Failure to provide the information necessary for the delivery of a Prize may result in delayed Prize delivery, disqualification of the Winner, or forfeiture of a Prize.
- 11.4. The Organizer shall have the right to make a Prize substitution of equivalent or greater value. The Organizer will not award a Prize if no eligible Submissions are entered in the Challenge.

- 11.5. Winners are responsible for any fees associated with receiving or using a Prize, including but not limited to wiring fees.
- 11.6. Winners are responsible for reporting and paying all applicable taxes in their jurisdiction of residence. The Organizer reserves the right to withhold a portion of the prize amount to comply with the relevant tax laws.
- 11.7. In case there are no Winners the Prizes will be awarded within the same ranking based on the quality and rigor of the procedures followed, as determined by a team of experts of the Organizer.
- 11.8. In case there are from 1 to 3 Winners the null Prizes will be shared equally among the other winners.
- 11.9. If several participants tie after the tie-breaking technique, the prize for the corresponding position will be shared equally among the tied participants.

12. Termination

- 12.1. The Organizer may terminate your participation in the Challenge in writing (by email) if you breach these Terms. This termination will take effect immediately after such termination email has been sent.
- 12.2. We shall not be liable to you or any third party for any claims or damages arising out of any termination or suspension, or any other actions taken by the Organizer in connection therewith.
- 12.3. Participants may drop out of the Challenge and forego any further participation. However, they will not be able to retract their prior submissions till that point in time.

13. Miscellaneous

- 13.1. If a virus, bug, bot, catastrophic event, or any other unforeseen or unexpected event that cannot be reasonably anticipated or controlled (also referred to as *force majeure*) affects the fairness and integrity of the Challenge, the Organizer has the right to cancel, change, or suspend the Challenge. This right is reserved whether the event is due to human or technical error. If a solution cannot be found to restore the integrity of the Challenge, the organization reserves the right to select Winners from among all eligible Submissions received before the Challenge needs to be cancelled, changed or suspended.
- 13.2. If any Participant attempts to compromise the integrity or the legitimate operation of the Challenge by cheating or committing fraud in any way, the Organizer may claim damages to the fullest extent permitted by law.
- 13.3. The Organizer reserves the right to modify these Terms at any time, without warning or notice, and to suspend, withdraw or cancel the Challenge for any reason and at any time, at its sole discretion and without incurring any liability.
- 13.4. The execution of the Challenge and the interpretation and enforcement of these Terms shall be exclusively governed by and construed by the laws of Spain. Any conflict regarding the Challenge or these Terms shall be subject to the exclusive jurisdiction of the courts of Spain.
- 13.5. If you have any questions about these Terms, please get in touch with us via mail through reid_challenge@iislafe.es .

----- Please add the following information -----

I agree to the above Terms.

Full name of Participant: _____

Username: _____

Institution's full name: _____

Ethical considerations, if applicable: _____

Your Institutional email: _____

Digital signature:

Date: __/__/2024.

I participate¹: Individually In a Team

If you participate as part of a Team, please add the following information:

Name of the Team²: _____

Full name(s) of the other Team member(s)	Email(s) of the other Team members(s)	Signature of the other Team members(s)

¹ Cross, or mark in any other way, the applicable option.

² Please, only include lowercase letter and numbers. Do not use any special characters or spaces in the team's name.

Annex I – UPV Platform Security Measures

Accessing the Intercambio Service means that you are a Data User

If you provide a service by virtue of an employment relationship in a public or private legal person, your organisation is considered as the data user. If your access purpose is providing a service to third parties, you are responsible for complying with these terms and conditions.

In such a case, it is assumed that legal representative or a natural person who has been delegated the power of attorney for such acceptance has requested the access and the acceptance of the terms and conditions of use of the Intercambio Service provided by UPV platform.

During your work in our information system, you must individually guarantee that you are aware of and accept our forbidden activities and mandatory security measures:

A. Forbidden activities:

The following purposes or processing activities are prohibited:

- (a) taking decisions detrimental to a natural person based on their electronic health data; in order to qualify as “decisions”, they must produce legal effects or similarly significantly affect those natural persons;
- (b) taking decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract or to modify their contributions and insurance premiums;
- (c) advertising or marketing activities towards health professionals, organisations in health or natural persons;
- (d) providing access to, or otherwise making available, the electronic health data to third parties not mentioned in the data permit;
- (e) developing products or services that may harm individuals and societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco products, or goods or services which are designed or modified in such a way that they contravene public order or morality;
- (f) using the data for purposes other than those stated in the request;
- (g) any act of misappropriation of the data, including the copying of the data on own premises, consultation by unauthorised persons or any conduct in breach of the conditions granted for access to the data;
- (h) failure to comply with obligations under these terms and conditions and any specific conditions to which a particular access authorisation may be subject;

(i) any conduct contrary to the law, fundamental rights or public order that according to the applicable legal framework is prohibited and/or constitutes an administrative infringement or a criminal offence.

B. Obligations

The authorised Data User shall:

- (a) use the Data on the terms and for the purposes expressly authorized;
- (b) Privacy-related obligations.
- (c) comply with security measures;

1. Privacy-related obligations

User will take the following steps in order to protect the privacy rights of all individuals whose images are included within the Dataset:

- a. User will not use the Dataset, either alone or in concert with any other information, to contact individuals who are or may be the sources of the information in the Dataset without specific written approval from the Responsible of the challenge.
- b. User will not request, and the Data Responsible of the data will not release, the key codes to the Dataset to the User. Further, User will not request the key codes from any third parties that provided the Dataset to the Data Responsible.
- c. User will follow relevant institutional policies and applicable European and national laws and regulations (if any) concerning the completion of ethics review or approval that may be required for the Project.

2. Security obligations (including confidentiality and data breach procedure)

The Intercambio Service has appropriate security measures in place. It automatically erases stored information after 20 days or upon file download completion, ensuring timely deletion. Access to the platform is personalized, limiting access to authorized individuals/teams. Additionally, information is downloaded through a single-access link, preventing unauthorized access after the initial download.

As a user of an information system, you must comply with all security obligations that have been expressly notified to you and in particular:

- You accept that any of your activities in the platform including your access is traceable. In this way, **your activity will be logged.**
- Both, with regard to ensuring the security of the platform and the implementation of security measures to prevent unauthorised access to the

platform, you agree to maintain confidentiality and to ensure the security of the data, obligations that shall continue to apply even after the termination of your relationship with the use of the platform.

- All the information is considered confidential.
- The media or equipment that you will use is managed by your organisation and it is a task of your organisation/company the guarantee of adequate security of such equipment.
- The equipment used to access the platform will implement physical and logical access controls including measures like:
 - Password for computer use, which must not be stored in readable files, macros, or any other place where they can be accessed by unauthorised people.
 - In the case of user absence from the working place, the workstation/laptop must be locked, which must in any case occur automatically after 15 minutes of inactivity.
 - The screen computer position shall ensure that showed information is not accessible or legible to unauthorised people.
 - The computer shall be switched off at the end of the working period and shall not be used by unauthorised people.
 - Computer media containing protected information (like access credentials or just temporal information or pictures saved in cache) may not be donated to any third party without first having been completely and securely erased.
 - The user is responsible for Internet access that may compromise the security of its equipment.
 - Users must keep the operating systems, antivirus and firewalls of their work equipment updated.
- **Any security breach must be communicated urgently** to:
 - Breaches just related to security
 - security.chaimeleon-eu@i3m.upv.es
 - Security breaches that could involve privacy data
 - dpdchaimeleon@irtic.uv.es
 - Specifically when this involves:
 - A possible platform access credential stolen or lost.
 - A laptop with saved credential access stolen or lost.
 - Any incident that, in the user opinion, could put the platform at risk.

Responsibility

Violations of the obligations of these obligations or the legal framework generate liability and/or responsibilities. The Responsible of the platform may notify the authorities of such violations when it has a legal duty to do so.

The Universidad Politécnica de Valencia acts exclusively as a communication service provider between the parties, and is not responsible for the contents that, in contravention of its Regulations for the Use of Computer Services and Resources, the users of this File Exchange Service may send to each other, and the users are solely responsible for the veracity and legality of the same. In particular, the use of this service for the remission of illegal content of any kind and, particularly, content that violates any patent, trademark, trade secret, copyright or any other property right is prohibited.

Annex II – UPV Platform Privacy Policies

1. For what purposes do we collect your personal information?

We will process your data in order to the:

- Administrative management of requests for access and use of data from the Dataset.
- Management of the security of the Dataset.
- Attention to requests from the interested public.

2. Who is the data controller?

Description of CHAIMELEON Joint Controllership

- ((1) Instituto de Investigación Sanitaria La Fe - Fundación para la Investigación del Hospital Universitario la Fe de la Comunidad Valenciana, established in Avenida Fernando Abril Martorell 106, Torre A, Planta 7ª, 46026 Valencia, Spain, VAT number: ESG97067557 (HULAFE);
- ((2) Università di Pisa, established in Lungarno Pacinotti 43/44, Pisa 56126, Italy, VAT number: IT00286820501 (UNIFI);
- ((3) Università degli Studi di Roma La Sapienza, established in Piazzale Aldo Moro 5, Roma 00185, Italy, VAT number: IT02133771002 (ULS),
- ((4) Unidade Local de Saúde de Santo António, EPE (before Centro Hospitalar Universitário De Santo António EPE) established in Largo Professor Abel Salazar, Porto 4099 001, Portugal, VAT number: PT517392259 (ULSSA);
- ((5) Policlinico San Donato SPA, established in Via Rodolfo Morandi 30, San Donato Milan 20097, Italy, VAT number: IT05853360153 (PSD);
- ((6) Collège des Enseignants de Radiologie de France, established in Rue De La Colonie 47, Paris 75013, France, VAT number : FR28387734775 (CERF);
- ((7) Universiteit Maastricht, established in Minderbroedersberg 4-6, Maastricht 6200 MD, Netherlands (UM); VAT number: NL 003475268B01
- ((8) Charité – Universitätsmedizin Berlin, established in Chariteplatz 1, Berlin 10117, Germany, VAT number: DE228847810 (CHARITE);
- ((9) Imperial College of Science Technology and Medicine, established in South Kensington Campus Exhibition Road, London SW7 2AZ, United Kingdom, VAT number: GB649926678 (IMPERIAL);
- ((10) Ben-Gurion University of The Negev, established in Beer Sheva 84105, Israel, VAT number: IL500701644 (BGU);
- ((11) Universitat Politècnica De Valencia, established in Camino De Vera s/n Edificio 3A, Valencia 46022, Spain, VAT number: ESQ4618002B (UPV);
- ((12) GE Healthcare GMBH - GEHC, established in Beethoven Strasse 239, Solingen 42655, Germany, VAT number: DE238938711 (GEHC);
- ((13) QUIBIM SL, established in EDIFICIO EUROPA, Av. d'Aragó, 30, Planta 13, 46021, Spain, VAT number: ESB98481658 (QUIBIM);
- ((14) MEDEXPRIM, established 815 La Pyrénéenne, 31670 LABEGE, France, VAT number: FR95814667267 (MEDEXPRIM);
- ((15) Bahia Software SL, established in Rua Das Hedras 4, Bloque 1, Planta Bajo Poligono Novo Milladoiro, Ames A Coruna 15895, Spain, VAT number: ESB15682594 (BAHIA);
- ((16) EIBIR Gemeinnützige GMBH Zur Forderung Der Erforschung Der Biomedizinischen Bildgebung, established in NEUTORGASSE 9/2, WIEN 1010, Austria, VAT number: ATU62615557 (EIBIR);

3. Are data transferred to a non-EU Country?

No international data transfers are foreseen.

4. How long do we keep/storage your data?

The data shall be processed for the duration of the research for the necessary period of time in accordance with the following criteria:

- During the period of the data access permission it will be kept active and in use.
- After the end of this period, the data will be kept exclusively for auditing and control purposes for the entire life cycle of CHAIMELEON Project and, in any case, for the period of the prescription of possible legal liabilities (data limitation). During this period, the personal data will be used exclusively for audit and control purposes or at the request of law enforcement authorities.

The information shall be kept suitably blocked for such additional periods as may be necessary for the prescription of possible legal liabilities including those arising from audits of the Project.

Data may be preserved indefinitely in accordance with legislation on historical or documentary heritage and/or archiving.

5. How do we protect the security of your information?

The corresponding technical, organisational and operational security and data protection measures are applied in accordance with the Spanish National Security Scheme.

In case of outsourcing of services, we will require and ensure that the processor applies measures analogous to those of the National Security Scheme.

6. How can you exercise your rights?

In order to maintain control over your data at all times, you have the right to access your personal information, as well as the right to request the rectification of inaccurate data or, where appropriate, to request its erasure or deletion. In certain circumstances, and for reasons relating to your particular situation, you may object to the processing of your data. Similarly, you may exercise the right to restrict the processing of your personal information, requesting its retention, as well as the portability of your data.

The exercise of rights is personal and therefore we need to identify you unequivocally. You can exercise your rights in two ways:

- By sending an e-mail message.

To do so, please use this address: dpdchaimoleon@irtic.uv.es

We will only deal with requests made from e- mail accounts provided in our databases after the identification of its owner.

- Physically by writing to the address of the data controller.

Mr. Ricard Martínez.

CHAIMELEON PROJECT DATA PROTECTION OFFICER

IRTIC-Universitat de Valencia

c/ Catedrático José Beltrán, 2.

46980 Paterna (Valencia), Spain.

In this case, you must provide supporting documentation:

- Proof of the identity of the person concerned by means of any valid document, such as identity card or passport.
- Name and surname of the person concerned or, where appropriate, of the person representing him/her, and the document proving such representation.
 - The request you are applying for.
 - Documents supporting the request you are making, if applicable.
 - In case of rectification or erasure, indication of the data to be rectified or erased and the reason for the rectification or erasure.
 - Address for delivery to you the information or notification.
 - Date and signature of the applicant.

7. Who guarantees your rights and to whom can you complain?

If you wish to lodge a complaint or obtain further information about the regulation of the processing of personal data in Spain, the competent authority is the Spanish Data Protection Agency (Agencia Española de Protección de Datos, Jorge Juan, 6 28001-Madrid).