

PRIVACY POLICY

Cyprus Cancer Research Institute (C.C.R.I.)

1. Scope

Cyprus Cancer Research Institute (C.C.R.I.) (hereafter CCRI) has a wide range of functions as an organisation, ranging from research, education, human resources and more. Almost all these functions require CCRI to use data about living individuals to deliver them.

To use personal data, CCRI must comply with the relevant General Data Protection Regulation (GDPR) – Regulation (EE) 2016/679 and all its amendments and as is enacted by Cyprus Law (N125(1)/2018) and all its amendments.

The purpose of this Privacy Policy is to outline why, how and which personal data is collected by the CCRI and what we do with it. In addition, this Privacy Policy gives you information about your relevant rights, how to obtain further information or lodge a request or complaint regarding your personal data held by CCRI.

2. Some information about key terms

We, us, our, CCRI, Institute - This privacy policy is issued on behalf of CCRI so when we mention “we”, “us” “our” or “CCRI” in this privacy policy, we are referring to Cyprus Cancer Research Institute (CCRI).

Personal information - Data that relates to a living individual who can be identified from this data, or from a combination of this data and other data which is in the possession of, or is likely to come into the possession of, the Data Controller.

Special category personal data - sensitive personal data, such as information about one’s race, ethnic origin (nationality), political views, religious beliefs, sexual life, trade union membership, physical or mental health or condition, genetic or biometric data or commission of offence/criminal records.

Data Subject - The living individual to whom identifiable personal data relates to, is called the Data Subject.

Data controller - Individual or organisation who determines the purposes for which and the lawful manner in which any personally identifiable data is or will be processed. In most cases when your personal data is collected for purposes and services relating to CCRI the Institute will act as the Data Controller.

Data processor - Person or organisation (other than an employee of the Data Controller) who processes personal data on behalf of the Data Controller.

Data breach - Any failure to meet the requirements of the data protection laws, unlawful disclosure or misuse of personal data and an inappropriate invasion of people's privacy.

Anonymised data - Data to which a statistical technique has been applied to group them to reveal general trends/values without identifying individuals within the data.

3. When is collection and use of personal data allowed

Under the relevant laws CCRI can only collect and use personal information for legitimate reasons. A legitimate reason is when we have an academic, research or other business reason based on legal bases to use personal information, so long as this is not overridden by your own rights and interests.

Personal data can be collected only under the following legal bases:

- If we have the Data Subject's consent;
- When it is necessary to execute a contract with the Data Subject;
- Where it is necessary to facilitate compliance with a legal obligation;
- When processing is necessary in order to protect the interests of the Data Subject or of another person;
- For the execution of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- If a legitimate interest of the CCRI, Data Subject or others justifies so.

Special category personal data may be collected only when there is good reason and this will be communicated separately in advance. Special category personal data is collected and processed where:

- Explicit consent has been provided;
- Processing is essential to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving consent;
- Processing is necessary for reasons of substantial public interest, on the basis of European Union law or Cyprus law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- Processing is executed for medical diagnosis, the provision of health or social care or treatment;

- On the basis of European Union or Cyprus law or pursuant to contract with us and the Data Subject for the provision of relevant services.

4. What personal information might be collected and processed

The CCRI may collect and use the following data types, depending on the relationship and interaction you may have with the CCRI:

- **Identity data:** such as first and last names, date of birth, ID number and social security number, images from CCTV systems installed in our premises and other information that enables the C.C.R.I. to check and verify your identity;
- **Contact information:** such as billing address, delivery address, email address and telephone number;
- **Background information:** such as employment history, qualifications, social media accounts, profession, professional memberships, educational achievements, diplomas, transcripts, languages, computer skills, national service completion (if applicable), grades, references and any data provide in CVs, interviews, applications, cover letters, questionnaires, surveys, exams;
- **Browser data:** standard information that a web browser sends to every website visited (such as the IP address, browser type and language, access times and referring website addresses);
- **Cookies:** small bits of information that are stored by the browser on your computer. These cookies are used to store preferences and various other bits of information about users of the website. C.C.R.I. will used only strictly necessary cookies. Although you can turn off the use of cookies in your browser, this may make the website unusable;
- **Financial information:** such as card number, account number, IBAN number and other financial information (where payment by or to you may be required).
- **Sensitive data:** such as genetic profile, ethnicity, nationality, gender and information about medical (including results of tests, diagnosis, treatment, care regiment, allergies and side-effects of medication, scans and other) and mental health. This type of data will only be collected when explicit consent in given.
- **Research data:** such as any of the above that we must collect and process as defined by each research protocol and are being indicated in the consent forms signed by research participants.

Collecting and processing the data types as described above, usually takes place through:

- Direct interaction with CCRI (physical space and its agents);
- IT and security systems;

- Website and social media accounts;
- Subscription to our newsletters;
- Attendance to CCRI functions, events and other activities (whether in our physical space, web-based systems or third-party spaces procured to run such CCRI activities);
- Other professionals such as from the social, healthcare and other services (where applicable).

5. Why we collect and use personal information

Personal information may be collected due to your interaction with C.C.R.I., including as a:

- Visitor;
- Donor;
- Volunteer to any of our charity initiatives;
- Members of the public;
- Persons indicated as next of kin for an employee or student;
- Employee;
- Student;
- Collaborator;
- Research participant and a research participant's legal guardian where applicable;
- Candidate for recruitment;
- Supplier or contractor.

The list below outlines how your personal data may be used and processed by CCRI. For the indicated purposes below, one or more of the legal bases described above (section 3) may apply and a single or a combination of data types as described above (section 4) may be used:

- To provide our services;
- To manage our relationship with you;
- To execute employment or other contracts;
- To run, administer and protect our business;
- Gathering and providing information and making filings required by law or relating to audits, enquiries or investigations by regulatory bodies or authorities;
- External audits, quality checks and relevant information pursuant to the applicable Cyprus laws;
- To improve our website functionality;
- To contact your next to kin;
- For research purposed where informed consent was freely given;

6. Promotional communications

We may use your personal information to send you updates (by email, text message, telephone or post) about our services and activities, such newsletters, events etc.

We rely on your consent to send you promotional communications and we will ask for this consent separately and clearly.

Where you have provided your consent for promotional communications, you have the right to withdraw it at any time by:

- Emailing, calling or writing to you (see below: 'How to contact us').
- Using the 'unsubscribe' link in emails or 'STOP' number in text messages (where applicable).

We will always treat your personal information with the utmost respect and never share it with other organisations outside the C.C.R.I. for marketing purposes.

7. Where your personal information is held

Information may be held at our offices and those of our group companies, third party agencies, service providers, representatives and agents as described in the 'Who we share your personal information with' section.

8. Keeping your personal information secure

We have appropriate security measures to prevent personal information from being accidentally lost or used/accessed unlawfully. We limit access to your personal information to those who have a genuine business need to access it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

9. How long your personal information will be kept

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for (see section 5), including for the purposes of satisfying any legal, accounting, or reporting requirements.

More specifically, personal data collected:

- Under the legal basis of consent will be deleted when the Data Subject withdraws their consent (exceptions apply for data used for scientific and/or statistical purposes).
- Under the legal basis of the execution of a contract will be retained for the period required for the execution of the contract and subsequent requests, claims and/or interests.
- Under the basis of legal obligation will be retained for the period determined by the obligation itself.
- For any other reason will be retained only for the necessary period to fulfil the purpose the data has been provided for.

We will not retain your personal information for longer than necessary for the purposes set out in this policy or specific contractual agreements or consent. When it is no longer necessary to retain your personal information, we will delete or anonymise it.

10. Who we share your personal information with

We routinely share personal information with Data Processors such as:

- Affiliated organisations;
- Service providers such as third parties we use to help deliver our services. This could include but is not limited to payment service providers, hosting providers, licensing providers and delivery companies, insurers and banks;
- Other third parties we use to help us run our business, for example marketing agencies or website hosts;
- Third parties approved by you, for example social media sites you choose to link your account to or third-party payment providers;
- Professional advisers including lawyers, consultants and auditors who provide legal, consultancy and auditing services;
- Share patient data with health professionals directly involved with the research participants' care.

We only allow third parties to handle your personal information if we are satisfied, they take appropriate measures to protect your personal information. We also impose contractual obligations on service providers relating to ensure they can only use your personal information to provide relevant services.

We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations. We may also need to share some personal information with other parties, such as potential buyers of some or all our business or during a re-structuring. Usually, information

will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

11. Transferring your personal information out of the European Economic Area (EEA)

To deliver our services and activities, it is sometimes necessary for us to share your personal information outside the EEA, such as:

- With your and our service providers located outside the EEA;
- If you are based outside the EEA;
- Where there is an international dimension to the services or activities we provide.

These transfers are subject to special rules under European and Cyprus data protection laws. Whenever we transfer your personal information out of the EEA, we ensure a degree of protection similar to that afforded in EEA countries by ensuring at least one of the following safeguards is implemented:

- We will transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal information by the European Commission (for more information refer to https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 03-06-2020)).
- Where we transfer your personal information to countries that have not been deemed to provide an adequate level of protection for personal information by the European Commission, we may use specific contracts approved by the European Commission or specific and comprehensive non-disclosure agreements which give personal information the same protection it has in Europe.

12. Your rights

You have the following rights in relation to your personal information:

Informed - The right to know why, what and how your personal information is been collected, used and stored, by whom and whom it may be shared with.

Access - The right to be provided with a copy of your personal information.

Rectification - The right to require us to correct any mistakes in your personal information. This enables you to have any incomplete or inaccurate information we hold about you corrected, though we may need to verify the accuracy of the new information you provide to us.

To be forgotten - The right to require us to delete your personal information (in certain circumstances). This enables you to ask us to delete or remove

personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal information to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Restriction of processing - The right to require us to restrict processing of your personal information (in certain circumstances). This enables you to ask us to suspend the processing of your personal information in the following scenarios: (a) if you want us to establish the information's accuracy; (b) where our use of the information is unlawful but you do not want us to erase it; (c) where you need us to hold the information even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your information but we need to verify whether we have overriding legitimate grounds to use it.

Data portability - The right to receive the personal information you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party. This right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

To object - The right to object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal information for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Not to be subject to automated individual decision-making - The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you.

Note you can withdraw consent at any time where we are relying on consent to process your personal information. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

For further information on each of those rights, including the circumstances in which they apply, please contact us or visit the website of Commissioner for the Protection of Personal Data (www.dataprotection.gov.cy).

13. Changes to this privacy policy

We may change this privacy notice from time to time—when we do, we will post the updated privacy notice on our website along with a summary of the changes (see section 16).

14. How to contact us

Please contact us by post, telephone or email if you have any questions about this privacy policy or the information, we hold about you.

Data Subject s can exercise any one and all of their rights by submitting a **Data Subject Access Request Form** to:

A) By post to:

Cyprus Cancer Research Institute (CCRI)
1 University Avenue, 2109, Aglangia, Nicosia, Cyprus
For the attention of the Data Protection Officer

B) Directly calling or emailing the Data Protection Officers:

Martha Trichina and Christiana Papamichael
E-mail: dpo@ccri.org.cy
Telephone: +357 22 89 43 76

Along with the completed **Data Subject Access Request Form**, we also require evidence of your identity. Please provide a photocopy or scan of an approved form of photographic evidence of your identity. Examples include a photo ID card or your passport ID page.

CCRI aims to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made several requests. In this case, we will notify you and keep you updated.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

15. How to make a complain

We hope that we can resolve any query or concern you may raise about our use of your information.

If you are not satisfied with how your request had been handled, you have the right to lodge a complaint with a supervisory authority.

The supervisory authority in Cyprus is the Commissioner for Personal Data Protection who can be contacted by:

Post: P.O.Box 23378, 1682 Nicosia, Cyprus

Telephone: +357 22 81 845 6

Fax: +357 22 30 45 65

Email: commissioner@dataprotection.gov.cy

For further information and guidance on how to lodge a complaint please visit www.dataprotection.gov.cy.

16. Document control

This is a controlled document. Refrain from using photocopies as these may be out of date. If you need to refer to C.C.R.I. policies and other controlled documents, please access them through the pertinent document repository or website or by directly requesting them by emailing info@ccri.org.cy.

CURRENT DOCUMENT INFORMATION			
Document type	POL	Author	Christiana Papamichael Data Protection Officer
Document number	CCRI_2020_115	Approver	Board of Directors (BoD)
Document title	Privacy Policy	Approval date	5 th BoD meeting on 06-07-2020
Version number	1.0	Publishing date	06-08-2020
Version date	08-07-2020	Review due on	07-07-2022
VERSION HISTORY			
Version number	Version date	Summary of changes	
1.0	08-07-2020	Initial version	

ANNEX 1

DATA SUBJECT ACCESS REQUEST FORM Cyprus Cancer Research Institute (C.C.R.I.)

Under Cyprus Law (N125(1)/2018) all living individuals to whom identifiable personal data relates to (called data subjects) have several rights relating to their personal data that the CCRI holds. Exercising their rights can be done through the current Data Subject Access Request form.

1. Data Subject's Information

Please provide the information about whose data the request is about (i.e. who is the Data Subject):

Name:
National ID/Passport number:
Date of Birth:

Tick (✓) what best describes the Data Subject's relationship with CCRI:

Employee (current or past)		Supplier or contractor	
Student (current or past)		Volunteer	
Collaborator		Visitor	
Persons indicated as next of kin		Candidate for recruitment	
Research participant		Member of the public	
Other (please specify):			

2. Requestor's Information

ONLY COMPLETE THIS SECTION IF THE REQUEST IS BEING MADE BY AN INDIVIDUAL OTHER THAN THE DATA SUBJECT.

These details are required in order for CCRI to process the request:

Name:
National ID/Passport number:
Date of Birth:

Tick (✓) the premise under which you are making this request (please provide evidence):

Parental responsibility	
Legal representative	
Written authorisation by the Data Subject	

3. Contact details

Where responses to this request should be directed to:

Name:	Email:
Address:	Phone:

4. Reasons for making the request

Tick (✓) the right you wish to exercise by submitting this request. For a more detailed explanation about your relevant rights please refer to the CCRI Privacy Policy as found in on our website www.ccri.org.cy

Please note that certain rights are not absolute, for example if personal data is being processed/stored for scientific and/or statistical purposes the right to object is more limited. Any limitations will be explained to you in the response to your request.

Right to be informed (knowing how, why and what a Data Subject's personal data is collected and used for)	
Right to access (obtaining a copy of a Data Subject's personal data)	
Right to rectification (correcting a Data Subject's personal data)	
Right to be forgotten (deleting a Data Subject's personal data)	
Right to restrict processing (limit use but allow storage of a Data Subject's personal data)	
Right to portability (transferring and reusing a Data Subject's personal data across other services)	
Right to object (stop processing/ withdrawing consent relating to a Data Subject's personal data)	

Provide further details about your request. For example if you require specific documents/files, let us know which departments may hold these and include any relevant dates or if you would like to let us know the reasons for making this request please include them here.

5. Identification evidence

Tick (✓) to indicate which proof of identity you will supply:

National ID card	
-------------------------	--

Passport	
----------	--

6. Declaration

- I certify that the information given in this request to the CCRI is true.
- I agree that the personal information I provided herein is necessary for the CCRI to confirm my identity and it may be necessary to obtain more information.
- I willingly supply along with this form a photocopy or scan of my National ID card or Passport as a form of photographic evidence of my identity,

Signature:

Date:

7. Submitting your request

Send your completed form and related evidence of identity:

C) By post to:

Cyprus Cancer Research Institute (CCRI)

1 University Avenue, 2109, Aglangia, Nicosia, Cyprus
For the attention of the Data Protection Officer

D) By emailing the Data Protection Officer:

E-mail: dpo@ccri.org.cy