Privacy Policy

Last updated: April 2, 2024

1. Interpretation and definitions
    a. Interpretation

For the General Data Protection Regulation (GDPR), chAIron SA (chAIron, the Company, We, Us, or Our) is the Data Controller.

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or plural.

    b. Definitions

For this Privacy Policy:

- Company (the Company, We, Us, or Our, in this Agreement): refers to chAIron SA, registered at Rue De La Grotte 6, 1300 Lausanne.
- Cookies: small files that could be placed on your computer, mobile device, or any other device by a website, containing the details of your browsing history on that website among its many uses.
- Country: refers to Switzerland.
- Data Controller: the GDPR considers the Company as the legal entity that alone or jointly with others determines the purposes and means of the processing of Personal Data.
- Device: means any device that can access the service such as a computer, a mobile phone, or a digital tablet.
- GDPR: a European Union regulation on information privacy in the European Union and the European Economic Area, i.e., Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016, on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Personal Data: any information that relates to an identified or identifiable individual, such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity.
- Service: refers to the Website.
- Service Provider: any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service, or to assist the Company in analysing how the Service is used. For the GDPR, Service Providers are considered Data Processors.
- Usage Data: refers to data collected automatically, either generated using the Service or from the Service infrastructure itself (e.g., the duration of a page visit).
- Website: refers to chairon.io, accessible from https://chairon.io

- You: the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.
- Under GDPR, You can be referred to as the Data Subject or as the User as you are the individual using the Service.

2. Introduction

chAIron SA (hereinafter referred to as “chAIron”) is dedicated to upholding privacy and safeguarding personal data per pertinent privacy legislation, including the General Data Protection Regulation (GDPR) and other relevant data protection laws. This Privacy Policy establishes guidelines, directives, and internal protocols to ensure strict adherence by chAIron employees, contractors, and collaborators to the highest standards of data privacy and security.

This Privacy Policy delineates the policies and procedures governing the collection, use, and disclosure of user information when accessing the Service. It also informs users about their privacy rights and the legal protections afforded to them.

chAIron may utilize Personal Data to enhance and optimize the Service. By utilizing the Service, users consent to the collection and utilization of information under this Privacy Policy.

The company specializes in delivering clinical and strategic services, including the analysis and advice of pharmaceutical and biotechnological companies' assets. This involves the utilization of real-world data, advanced artificial intelligence models, and human expertise to advance the understanding of molecules for treating human diseases. Furthermore, the company collaborates with technological partners to predict and optimize clinical trial outcomes, thereby enhancing the efficacy of trial protocols. It is imperative to note that these models operate without reliance on personal information, focusing on experimental protocols and criteria tailored to specific needs without necessitating the processing of identifiable personal data.

During its activities and collaborations, the company may encounter and process information that may be related to personal information or deemed as personal information under specific regulations. In this context, it is crucial to highlight that the company predominantly utilizes de-identified information validated by a reputable provider in the field for research purposes, adhering to the provisions of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

Notwithstanding the above, in the company's operations, encompassing communication with clients, marketing activities, and employee recruitment, certain information may be classified as Personal Data. This policy serves as a guiding framework outlining the principles and practices related to privacy and data protection within the company.

3. Scope

This policy applies to all employees, contractors, and collaborators of the company who handle personal data in their work. Personal data includes any information that relates to an identified or identifiable individual, such as names, addresses, email addresses, phone numbers, and health-related data, to the extent exists, is accessed, or processed by the company.

4. Responsibilities

All employees, freelancer employees, and collaborators of the company are responsible for:

- Complying with this Privacy Policy and related procedures.
- Reporting any suspected data breaches or privacy concerns to the Data Protection Officer (DPO).
- Participating in privacy training and awareness programs provided by the company.

5. Data Protection Officer (DPO)

chAIron SA has designated a Data Protection Officer (DPO) to oversee and ensure compliance with this Privacy Policy and relevant privacy legislation. The DPO assumes a pivotal role in ensuring the company's unwavering commitment to data privacy and protection. The DPO is responsible for:

- Informing and Advising on Privacy Regulations
  The DPO serves as a beacon of knowledge, keeping the company apprised of its obligations under applicable privacy regulations. By providing informed advice, the DPO enables the company to navigate the intricate landscape of privacy laws with precision.
- Identification and Guidance on Data Processing Activities
  Meticulously identifying processing activities involving personal data, the DPO offers strategic guidance and instructions to ensure the company's handling of such data is not only proper but also fortified with robust security measures.
- Monitoring and Ensuring Compliance
  Vigilantly monitoring compliance with both applicable privacy regulations and the company's internal data protection policies, the DPO undertakes initiatives such as awareness-raising, training, and audits. This proactive approach reinforces a culture of data protection throughout the organization.
- Cooperation with Data Supervisory Authorities
  Acting as a liaison with data supervisory authorities, the DPO ensures transparent communication and collaboration on behalf of the company, thereby fostering a cooperative and compliant relationship with regulatory bodies.
- Data Subject Interaction and Inquiry Handling
  As the designated point of contact for data subjects, the DPO addresses inquiries related to the company's data processing activities. By facilitating transparent communication, the DPO contributes to building and maintaining trust between the company and individuals.
- Privacy Risk Assessment and Compliance Monitoring
  Upholding a proactive stance, the DPO oversees the performance of initial and periodic information privacy risk assessments. This includes conducting ongoing

compliance monitoring activities to identify and address potential risks promptly.

- Management of Data Incidents
  Ensuring a swift and effective response to data incidents, the DPO manages the process comprehensively. This includes filing required reports under applicable privacy regulations and fostering resilience in the face of unforeseen events.
- Legal Compliance and Technological Adaptation
  Staying abreast of the ever-evolving landscape of international, federal, and state privacy laws and accreditation standards, the DPO, either directly or through legal advisors, ensures the company's compliance. Moreover, the DPO monitors advancements in information privacy technologies to facilitate the company's adaptive and cutting-edge approach to data protection.

6. Privacy Principles

The Company adheres to the following privacy principles in its handling of Personal Data:

- Lawfulness, fairness, and transparency: personal data must be processed lawfully, fairly, and transparently.
- Purpose limitation: personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Data minimization: personal 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.
- Storage limitation: personal data must be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed.
- Integrity and confidentiality: personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage. Those principles are demonstrated within the company’s set of policies and procedures, as well as in the company’s analysis, mapping, and mitigation when processing data which was derived from personal data.

7. Collecting and Using Your Personal Data

The company shall ensure that any time personal data is being collected or processed:

- Personal data is collected and processed only for legitimate purposes. Where such data is collected for the delivery of services and is health-related, such data will always be de-identified before being used, unless explicit lawful consent was obtained as instructed by the Company’s legal advisors.
- If known, data subjects are informed about the purposes of data collection, the legal basis for processing, their rights, and any recipients or categories of recipients of the personal data.
- Consent is obtained from data subjects when required by law.

- Privacy impact assessments are conducted when necessary to identify and mitigate privacy risks associated with new projects, technologies, or processes.

While using Our Service, We may ask You to provide Us with certain personally identifiable information that can be used to contact or identify You. Personally identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Usage Data

Usage Data might be collected automatically when using the Service. Usage Data may include information such as Your Device's Internet Protocol (IP) address (e.g., IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device's unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

The Company may use Personal Data for the following purposes:

- To provide and maintain our Service, including monitoring the usage of our Service.
- To contact You: to contact You by email or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products, or contracted services, including the security updates, when necessary or reasonable for their implementation.
- To provide You with news, special offers and general information about other goods, services, and events which we offer that are like those that you have already purchased or enquired about.
- To manage Your requests: to attend and manage Your requests to Us.
- For business transfers: We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.
- For other purposes: We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns, and evaluating and improving our Service, products, services, marketing, and your experience.

We may share Your personal information in the following situations:

- With Service Providers: We may share Your personal information with Service Providers to monitor and analyse the use of our Service, to contact You.
- For business transfers: We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.
- With Affiliates: We may share Your information with Our affiliates, in which case we will require those affiliates to honour this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners, or other companies that We control or that are under common control with Us.
- With business partners: We may share Your information with Our business partners to offer You certain products or services.
- With other users: when You share personal information or otherwise interact in public areas with other users, such information may be viewed by all users and may be publicly distributed outside.
- With Your consent: We may disclose Your personal information for any other purpose with Your consent.

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer periods.

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to – and maintained on – computers located outside of Your state, province, country, or other governmental jurisdiction where the data protection laws may differ from those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and per this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

You have the right to delete or request that We assist in deleting the Personal Data that We have collected about You.

Please note, however, that We may need to retain certain information when we have a legal obligation or lawful basis to do so.

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g., a court or a government agency).

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation.
- Protect and defend the rights or property of the Company.
- Prevent or investigate possible wrongdoing in connection with the Service.
- Protect the personal safety of Users of the Service or the public.
- Protect against legal liability.

8. Data Storage and Security

The Company maintains appropriate technical and organizational measures to protect personal data (and any other sensitive data) against unauthorized or unlawful processing and accidental loss, destruction, or damage. These measures are further detailed in the Company's security procedures and include:

- Secure storage and transmission of personal data.
- Regular security audits and updates to software and hardware.
- Restricted access to personal data on a need-to-know basis.
- Security training and awareness programs for employees, contractors, and collaborators.

While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security.

9. Data Breach Response and Notification

In the event of a personal data breach, the Company has established procedures to:

- Investigate and contain the breach to prevent further unauthorized access, disclosure, or damage.
- Notify the DPO and CEO and nominate a designated team who will coordinate the response and determine whether the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Notify affected data subjects and supervisory authorities when required by law, providing information about the nature of the breach, the steps taken to address it, and the measures taken to mitigate its potential adverse effects.
- Document the breach, including its facts, effects, and remedial actions taken.

10. Data Subject Rights

The Company respects the rights of data subjects under applicable privacy laws, including the right to access, rectify, erase, restrict processing, object to processing, and data portability. Data subjects may exercise their rights by contacting the DPO. The company shall address data subject inquiries following its designated procedures, setting a clear easy-to-follow organizational flow ensuring that any such inquiry will be dealt with efficiently.

11. Data Retention and Destruction

The Company retains Personal Data only for the period necessary to fulfil the purposes for which it was collected or as required by law. Personal data that is no longer needed is securely destroyed or anonymized per established data retention and destruction procedures. Retention periods shall be defined clearly in the company's mapping documentation.

12. GDPR Privacy

We may process Personal Data under the following conditions:

- Consent: You have given Your consent for processing Personal Data for one or more specific purposes.
- Performance of a contract: provision of Personal Data is necessary for the performance of an agreement with You and/or for any pre-contractual obligations thereof.
- Legal obligations: processing Personal Data is necessary for compliance with a legal obligation to which the Company is subject.
- Vital interests: processing Personal Data is necessary to protect Your vital interests or those of another natural person.
- Public interests: processing Personal Data is related to a task that is carried out in the public interest or the exercise of official authority vested in the Company.
- Legitimate interests: processing Personal Data is necessary for the legitimate interests pursued by the Company.

In any case, the Company will help to clarify the specific legal basis that applies to the processing, and whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter a contract.

The Company undertakes to respect the confidentiality of Your Personal Data and to guarantee You can exercise Your rights.

You have the right under this Privacy Policy, and by law if You are within the EU, to:

- Request access to Your Personal Data. The right to access, update or delete the information We have on You. Whenever made possible, you can access, update, or request the deletion of Your Personal Data directly within the Service. If you are unable to perform these actions yourself, please contact Us to assist You. This also enables You to receive a copy of the Personal Data We hold about You.
- Request correction of the Personal Data that We hold about You. You have the right to have any incomplete or inaccurate information We hold about You corrected.

- Object to processing of Your Personal Data. This right exists where We are relying on a legitimate interest as the legal basis for Our processing and there is something about Your situation, which makes You want to object to our processing of Your Personal Data on this ground. You also have the right to object where We are processing Your Personal Data for direct marketing purposes.
- Request the erasure of Your Personal Data. You have the right to ask Us to delete or remove Personal Data when there is no good reason for Us to continue processing it.
- Request the transfer of Your Personal Data. We will provide to You, or to a third party You have chosen, Your Personal Data in a structured, commonly used, machine-readable format. Please note that 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.
- Withdraw Your consent. You have the right to withdraw Your consent to Us using your Personal Data. If You withdraw Your consent, We may not be able to provide You with access to certain specific functionalities of the Service.

You may exercise Your rights of access, rectification, cancellation, and opposition by contacting Us. Please note that we may ask You to verify Your identity before responding to such requests. If You make a request, We will try our best to respond to You as soon as possible.

You have the right to complain to a Data Protection Authority about Our collection and use of Your Personal Data. For more information, if You are in the European Economic Area (EEA), please contact Your local data protection authority in the EEA.

13. Children's Privacy

Our Service does not address anyone under the age of 21. We do not knowingly collect personally identifiable information from anyone under 21. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 21 without verification of parental consent, We take steps to remove that information from Our servers.

14. Changes to this Privacy Policy

We may update this Privacy Policy whenever there are significant changes to privacy legislation or chAIron's data processing activities. Updates will be communicated to all employees, relevant contractors, and collaborators, who are expected to adhere to the revised policy.

Changes will be posted on this page, and We will update the "Last updated" date at the top of this Privacy Policy. You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when posted on this page.

15. Compliance and Enforcement

Failure to comply with this Privacy Policy may result in disciplinary action, including termination of employment or contractual relationship. Any concerns about non-

compliance should be reported to the DPO. By implementing and enforcing this Privacy Policy, chAIron demonstrates its commitment to maintaining the privacy and security of personal data following privacy legislation, including the GDPR and upholding the trust of data subjects and partners.

16. Contact Us

If you have any questions about this Privacy Policy, You can contact us by email at contact@chairon.io.