PRIVACY POLICY

Table of Contents

1. INTRODUCTION

This Privacy Policy is issued on behalf of Sinclair Pharma Ltd. and its group companies ('Sinclair', 'us', 'we'). It's intended for users of Sinclair products & services, customers, providers, website visitors and for anyone interested in contacting with Sinclair.

Sinclair is a global medical aesthetics company, founded in the UK in 1971. Acquired by Huadong Medicine Ltd in 2018, we deliver an extensive product range. We provide an in-house commercial infrastructure, including manufacturing, company-owned affiliates, and a network of distributors in all leading global markets.

We collect, use and are responsible for certain personal data about you. When we do so we are subject to different data protection laws depending on the location of our customers and the provision of our services. Nevertheless, we are committed to deliver the highest standards in privacy protection regardless of where in the World you interact with us.

Please note that we may update this policy from time to time. We encourage you to review it periodically. This version is effective since February the 14th 2023.

Feel free to address our DPO if you need to review past versions of this document.

Please find all operative Sinclair entities & branches and our Data Protection Officer contact details listed below. In addition, to further guarantee the correct exercise of your data protection rights from outside the UK, we have appointed an EU Representative for any GDPR inquiries/ requests you may wisht to forward.

The Data Controller responsible for this website	**Identity:** SINCLAIR PHARMA LTD **Company. No.:** 3816616 **Address:** 30-32 Whitfield Street, Whitfield Court, London W1T 2RQ, United Kingdom. **Phone No.:** +44 (0) 20 7467 6920
Our Data Protection Officer **(DPO)**	If you have any queries or comments related to how we process your personal information, please contact our Data Protection Officer at: **Sinclair Data Protection Officer** Eden House, Lakeside, Chester Business Park, Chester Cheshire, CH4 9QT United Kingdom dpo@sinclair.com
SINCLAIR ('*us*', '*we*', *'our Group'*)	**UK**: Sinclair Pharma Ltd (Co. No.3816616), Sinclair Pharma Management Ltd (Co. No.9142486), Sinclair Pharma Holdings Ltd (Co. No.8871117), Sinclair Pharmaceuticals Ltd (Co. No. 1007146).

	EU & CH: SPL Belgian Branch (Co. No. 0834487832), Cocoon Medical International EOOD (Co.No.BG204280676), Sinclair Pharmaceuticals España SL (B-82861659), Sinclair Holdings Iberia SL (Co. No. 576995), High Technology Products SLU (B-62692603), Sinclair Pharma France Holding SAS (Co. No. 490245099), Sinclair France SAS (Co. No. 484283643), SPL French Branch (Co. No. 815253224), SPL Irish Branch (Co. No. 909183), Cocoon Medical Italy SRL (Co. No. IT11007360966), , Sinclair Pharma Gmbh (HRB 726234), Sinclair Pharma GmbH Zweignieder-lassung Gossau SG Swiss Branch (Co. No. 115621045), Sinclair Holding BV (Co. No. 29471362), AQTIS Medical BV (Co.No.20469853), Sinclair Netherlands IP BV (Co. No. 17368847), SPL Sp.z.o.o.Oddzial W Polsce (Co. No. 0000893589). **EU GDPR representative** *C/ Pau Claris, 154. 2° - 08009, Barcelona (SPAIN)* rep.eu@aurisadvocats.com **EURASIA**: SPL Russian Branch (Co. No. 9909565244). **MIDDLE EAST**: SPL UAE Branch (Co. No. 4038). **NORTH AMERICA**: Viora Ltd (Co. No. 513726091), Viora Canada Ltd (Co. No. 665279), Viora Inc (Co. No. 4337310), Cocoon Medical USA LLC (Co. No. 202005210387), Sinclair Pharma US Inc. (Co. No. C3054685). **PACIFIC ASIA**: Sinclair Pharma Australia Pty Ltd (Co. No. 631785398), Cocoon Medical Hong Kong Ltd (Co. No. 2794655), Sinclair Korea Ltd (Co. No. 110114-0207636), Sinclair Pharmaceuticals PTE Ltd (Co. No.202025226G), SPL Singapore Branch (Co. No. T15FC0070H). **SOUTH & CENTRAL AMERICA**: Building Health Distriubidora de Productos Para Saúde Ltda (Brazil Co. No 22577162/0001-20), Sinclair Chile SpA (Co. No. 16659409), Cocoon Medical Colombia SAS (Co. No. 2926001), Sinclair Aesthetics de Mexico (Co. No. 20180022098050049).

2. WHAT PERSONAL INFORMATION WE MAY COLLECT ABOUT YOU

We collect & process information about you every time we interact. You may provide the information directly or it may be provided by technical third parties, like Google or social media platforms. We may also gather information by using cookies. Please check our Cookies Policy.
Generally, you provide most of the personal information we collect directly. Either personally or by telephone, mail, web forms, contracts or by responding to our surveys. However, we may also collect personal information from:

- Third parties linked to us, such as:

i. A company within our group (please view our group companies above).
ii. A relevant third-party that has previously obtained your express consent to do so, such as your doctor, your bank, or your employer.

- From our information systems to access our premises if there are any. Such as, for example, entry and reception registers, CCTV.

The personal data we may collect and use, include:

- **Basic and contact information**: such as name, surname, username, or similar identifier. This category may include your billing and delivery address, email, and phone number.
- **Special category data:** only when strictly necessary we may process especially sensitive data related to your health, like possible side effects associated with one of our products or information you may provide to us during the course of our services from time to time.
- **Financial and economic data:** this category includes payment, return and reimbursement details as well as the commercial transactions you completed with us. This may include data to verify your identity for payment acceptance purposes to be able to perform commercial transactions with you.
- **Professional and employment data:** your job title, the company you work for and your relationship to a person.
- **Technical information:** like browsing data, including IP address, version and time zone usage, social media tracking pixels to allow platforms interact with our website and provide feedback, URLs clicked on, unique device identifiers, operating system, activity data, such as your login details and whether you completed our registration form.
- **User account data:** such as your profile name and password, history of subscriptions/purchases, information you provide when you create an account on our websites, subscribe to our service, request marketing to be sent to you, enter a competition or promotion, or register for a webinar. We also gather all your granted consents and your chosen communication preferences.
- **Image data**: footage that we may capture through our security video surveillance systems in our shops or premises.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract that we have with you and you fail to provide that data when requested, we may not be able to perform the contract or services. For example, such information may be needed to provide you with requested goods or services. In such instances, we may find it necessary to cancel a contract with you. We will previously notify you if this is the case.

3. HOW WE USE YOUR PERSONLA DATA: PURPOSES & LAWFUL BASIS

Purpose	Lawful basis for processing personal data
To provide you our services and products. This includes delivering orders to you, managing payments, fees, and charges, etc.	(1) Performance of a contract (2) Necessary for our legitimate interests (to recover debts due to us)
To improve and to update our products and services	(1) Necessary for our legitimate interests
To register you as a new customer or as web user	(1) Consent of the interested party (2) Performance of a contract
To manage our relationship with you which will include: (1) notifying you about changes to our Terms or Privacy Policy (2) asking you to leave a review or take a survey	(1) Performance of a contract with you (2) Necessary to comply with a legal obligation (3) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To send business mails, Newsletter, and advertisements through any communication form	(1) Performance of a contract (2) Necessary for our legitimate interests (providing you haven't expressed your desire to stop receiving, 'opt-out') (3) Consent of the interested party
To enable you to partake in a prize draw or competition, or complete a survey	Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to

effectiveness of the advertising we serve to you	grow our business and to inform our marketing strategy)
To use data analytics to improve your website experience, implement marketing strategies, improve customer relationships and purchasing experiences using cookies	(1) Necessary for our legitimate interests (2) Consent of the interested party (accepting our Cookie policy, for example)
To make suggestions and recommendations about products or services that may be of interest to you	Necessary for our legitimate interests (to develop our products/services and grow our business)
To prevent and detect fraud against you, us, or a company within our group	For our legitimate interests or those of a third party, i.e., to minimise fraud that could be damaging for us and for you
Collecting and providing information required by or relating to audits, enquiries, or investigations by regulatory bodies	To comply with our legal and regulatory obligations
Ensuring business policies are adhered to, i.e.,. policies covering security and internet use	For our legitimate interests or those of a third party, i.e., to make sure we are following our own internal procedures so we can deliver the best products/services
Operational reasons, such as improving efficiency, training, and quality control	For our legitimate interests or those of a third party, i.e., to be as efficient as we can so we can deliver the best products/services
Ensuring the confidentiality of commercially sensitive information	(1) For our legitimate interests or those of a third party, i.e., to protect trade secrets and other commercially valuable information (2) To comply with our legal and regulatory obligations
Preventing unauthorised access and modifications to our systems	(1) For our legitimate interests or those of a third party, i.e., to prevent and detect criminal activity that could be damaging for us and for you (2) To comply with our legal and regulatory obligations
Updating and enhancing customer records	(1) For the performance of our contract with you or to take steps at your request before entering into a contract

	(2) To comply with our legal and regulatory obligations (3) For our legitimate interests or those of a third party, i.e., making sure that we can keep in touch with our customers about existing orders and new products
Ensuring safe working practices, staff administration and assessments	(1) To comply with our legal and regulatory obligations (2) For our legitimate interests or those of a third party, i.e.,. to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
External audits and quality checks, i.e., for ISO or Investors in People accreditation and the audit of our accounts	(1) For our legitimate interests or a those of a third party, i.e., to maintain our accreditations so we can demonstrate we operate at the highest standards (2) To comply with our legal and regulatory obligations
Deciding about your recruitment or appointment. Determining the terms on your job with us, providing contractual benefits to you, pension plan arrangements, accounting, reviewing staff performance, education & training requirements, complying with health & safety obligations, equal opportunities monitoring, dealing with legal disputes involving staff, employees, and contractors, including accidents on our premises.	Necessary for our legitimate interests and to comply with our legal and regulatory obligations
To provide greater security to our facilities (installation of CCTV cameras / video surveillance, access control)	For our legitimate interests or those of a third party, i.e., to prevent harm over our employees and clients
To respond to queries and to provide information to the interested party, including sending of budget proposals	(1) Legitimate interest (2) Contract performance (3) Express consent (4) Legal obligation

Manage user interactions on our social networks	(1) To comply with our legal obligations, for example erasing offensive comments, racism, maintain respect in conversations, protect minors, etc. (2) In our legitimate interest (for example erasing advertisement for others)
To provide the Authorities with information whenever mandatory	Compliance with our legal obligations
To guarantee job security, personnel management, and the employability of candidates	(1) To comply with our legal obligations (2) In our legitimate interest and of others. To improve our job experience for our staff

4. SHARING YOUR PERSONAL INFORMATION WITH OTHERS

To manage our relationship with you, we will share your information with the Sinclair teams within our group that need to access it to perform their job.
We may share your personal information with the following:

- Other members of the Sinclair group of companies.
- Trusted third parties, such as: our agents and suppliers; partners who provide us with technology services, such as data analytics, hosting, and technical support; our professional advisors; auditors and business partners; regulators, governments and other third parties in connection with the re-organising or merging of all or part of our business. If a change happens to our business, the new owners may use your personal data in the same way as set out in this Policy.
- With law enforcement bodies whenever mandatory.

We have binding privacy agreements in place with all our trusted third parties. All our data processors must certify that data subject's rights will be guaranteed according to applicable privacy laws.

Third-party websites
From time to time on our websites we may provide links to websites or mobile applications that are separate to and not controlled by us. This Policy does not apply to those websites. Should you choose to visit those third-party domains, please review the legal and privacy statements posted on each website or mobile application to understand their privacy practices.

5. INTERNATIONAL DATA TRANSFERS

International data transfers are submitted to special rules governed by the principles of data protection laws. Whenever we transfer your data internationally, we will do so based on appropriate adequacy decisions, implemented Standard Contractual Clauses

(SCCs) or International Data Transfer Agreements (IDTA). We will make sure that your information remains safe.

We may transfer your data internationally, for example:

- To communicate with you or our suppliers when you are outside the EEA/ UK.
- When there is an international dimension in the products/services that we provide you.

6. HOW WE KEEP YOUR DATA SAFE

Sinclair takes the protection of your personal data very seriously. For this reason, we guarantee the implementation of appropriate security measures, controls, and technical & organizational measures to prevent your information from destruction, loss, change, communication, or any form of malicious access.

We limit the access to your data to authorized entities & personnel. We make sure to properly train all our staff, and all those involved in the processing of your personal information are subject to the duty of confidentiality.

Where we contract with third-parties or suppliers, data protection audits and written data processing agreements are in place. Our partners will only process your personal data in accordance with our strict instructions and ensuring the correct exercise of data protection rights. Personal information will be kept confidential and appropriate security measures to safeguard your data are enforced.

Additionally, we have corporate protocols in place to immediately react to a data security breach incident or suspicion. If necessary, we will notify you of it as well as the relevant data control authority, in accordance with current regulations.

Please note that if you forward information to us, the transmission of data may not be entirely secure, and you will do so at your own risk.

7. PERSONAL INFORMATION RETENTION PERIOD

We will keep your personal data throughout the duration of our relationship unless you state otherwise.

Retention periods are based on the requirements of different data protection laws, regulations, limitation periods for legal action and the purpose for which the information is collected and used. We categorise information and specify the applicable retention period in accordance.

When personal information is destroyed, paper-based information will be disposed of via confidential waste bins and digital information will be permanently deleted.

We have specific data retention policies available upon request. Please contact our DPO to inquire further on our retention policies.

8. YOUR DATA PROTECTION RIGHTS

Under certain circumstances, you may request to exercise your Data Protection Rights. You can enforce these rights by contacting us by email to gdpr@sinclair.com or dpo@sinclair.com; by sending a request in writing addressed to:

Sinclair Data Protection Officer

Eden House, Lakeside, Chester Business Park,
Chester
Cheshire, CH4 9QT
United Kingdom

Or, you may use our dedicated online form GDPR Request form.

When making a request to exercise your rights, please state your request clearly and the personal information you are concerned about. We may need to verify your identity by requesting a form of ID, or we may need clarification or further information before fulfilling your request. We will action your request in a prompt manner, within 30 days from the date of your request for requests under the GDPR and UK GDPR or 45 days for requests under the California Consumer Privacy Act.

Your data protection rights are:

Right of access	Allows the interested party to acknowledge and obtain information about their personal data submitted to processing.
Right to rectification	It allows to correct errors and modify the data that proves to be inaccurate or incomplete.
Right to erasure of your data	Allows data that turns out to be inadequate or excessive to be deleted.
Right to withdraw consent	The right of the interested party to not carry out the processing of their personal data or to cease it.
Restriction of personal data processing	Involves the marking of personal kept data, with the purpose of limiting its' future processing.
Right to portability of data	Facilitation of the data subject to processing to the interested party, so that he or she can transmit it to

	another person in charge, without impediments.
The right not to be subject to automated individual decisions (including the elaboration of profiles)	the right not to be the subject of a decision based on automated processing that produces effects or significantly affects the User.

Please note that these rights are not absolute, therefore, we may not be able to fulfil your request and may continue to process your personal information to the extent required or otherwise permitted by law, in particular in connection with exercising and defending our legal rights or meeting our legal and regulatory obligations.

Data subjects based in the US additionally have the right not to receive discriminatory treatment by Sinclair for the exercise of the privacy rights conferred by CCPA and the right to opt-out of the sale of personal information, however Sinclair will never exchange your personal data for money.

9. THE SUPERVISORY DATA PROTECTION AUTHORITY

If you wish to file a complaint about privacy issues with Sinclair, please address our appointed Data Protection Officer who will help you with the matter. But if you still wish to file a complaint, you have the right to address the relevant supervisory data protection Authority, such as the ICO in the UK or the AEPD in Spain, the CNIL in France, the BfDI in Germany, etc.

Please click here to find your relevant Data Protection Authority.

The Information Commissioner's Office (ICO)

Water Lane, Wycliffe House
Wilmslow - Cheshire SK9 5AF, UK
Tel. +44 1625 545 745
Website: https://ico.org.uk

10. HOW YOU CAN CONTROL YOUR PERSONAL INFORMATION – OPTING OUT

If you currently receive marketing emails from us and no longer wish to do so you can unsubscribe within any such email. This opt out will not apply to personal information provided to us as a result of a product/service purchase, warranty registration, product/service experience or where otherwise permitted by law. Please see section 'Your data protection rights' above for further information on enforcing your rights.

You can choose to decline all non-essential cookies via the cookie banner on our website. If you accept cookies but later wish to withdraw consent, you can do so via the cookie widget in the bottom right corner of the site. If you decline cookies, please

note that some parts of our websites may not function properly. For more information about the cookies we use, please see our Cookies Policy.

11. HOW TO CONTACT US

If you have any questions, concerns, complaints or requests regarding this Policy, or if you would like to exercise any of the rights set out above, please let us know by contacting gdpr@sinclair.com or dpo@sinclair.com or by writing to the Sinclair contact address:

Sinclair Compliance Department
Eden House, Lakeside, Chester Business Park,
Chester
Cheshire, CH4 9QT
United Kingdom