

## PRIVACY NOTICE

**Last Updated on:** January 27, 2026

### General Information

#### 1. Keeping Your Insights Safe: Our Commitment to Secure and Reliable Data

ClinDART, Inc. (“ClinDART”, “we”, “us”, “our”) is dedicated to meeting our legal and ethical obligations when it comes to the processing of personal data as this term is defined under data protection and privacy laws (“Personal Data”). We are also dedicated to earning and maintaining your trust, and will continue to communicate about, manage, and protect Personal Data. This Privacy Notice (this “Notice”) explains how we collect, manage, use, transfer or otherwise process Personal Data. This Notice also explains how to contact us and what privacy rights you may have under applicable data protection and privacy laws.

#### 2. Information about ClinDART

ClinDART is a California corporation, providing custom data management and statistical programming, clinical trial management, and consulting services (collectively, the “Services”). ClinDART does not market its Services to individuals, **nor does ClinDART sell Personal Data.**

#### 3. Scope of this Privacy Notice

This Notice addresses Personal Data that we:

- process for our own business purposes in order to provide our Services, i.e., basic employment and contact information of business contacts from prospective and current customers (“Customers”);
- receive from our business partners; or
- process to promote our Services.

### Contents of this Notice

|           |  |   |
|-----------|--|---|
| <b>A.</b> | <b>What Is Not Covered by this Privacy Notice?</b>           | 2 |
| 1.        | Human Resources Personal Data                                | 2 |
| 2.        | Information Which Does Not Constitute Personal Data          | 2 |
| 3.        | Information We Process on Behalf of Customers                | 2 |
| <b>B.</b> | <b>Our Role with Respect to Your Personal Data</b>           | 2 |
| <b>C.</b> | <b>Collection of Personal Data and Purposes of Use</b>       | 3 |
| 1.        | Collection of Personal Data and Its Use                      | 3 |
| 2.        | How We Use the Data  | 3 |
| <b>D.</b> | <b>Lawful Bases for Processing</b>                           | 5 |
| <b>E.</b> | <b>International Transfers, Security, and Data Retention</b> | 6 |
| 1.        | International Transfers of Your Personal Data: Europe        | 6 |
| 2.        | Security   | 6 |

|           |  |    |
|-----------|--|----|
| 3.        | Data Retention .....   | 6  |
| 4.        | Right to Lodge a Complaint with a Supervisory Authority..... | 7  |
| <b>F.</b> | Cookies .....  | 7  |
| <b>G.</b> | Your Privacy Rights.....                                     | 7  |
| 1.        | What You Can Ask Us to Do.....                               | 7  |
| 2.        | Verification of a Consumer Request.....                      | 8  |
| 3.        | Response Timing and Format .....                             | 8  |
| 4.        | The Global Privacy Control and Do Not Track Signal.....      | 8  |
| <b>H.</b> | Children.....  | 9  |
| <b>I.</b> | Changes to Our Privacy Notice.....                           | 9  |
| <b>J.</b> | Contact Us.....  | 9  |
| 1.        | European Union Representative .....                          | 9  |
| 2.        | United Kingdom Representative.....                           | 10 |
| 3.        | Data Protection Officer .....                                | 10 |

#### **A. What Is Not Covered by this Privacy Notice?**

##### 1. Human Resources Personal Data

This Notice does not apply to the Personal Data of ClinDART employees, job applicants, contractors, business owners, directors, or officers.

##### 2. Information Which Does Not Constitute Personal Data

If we do not maintain information in a manner that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household, such information is not considered Personal Data, and this Notice will not apply to our processing of that information.

##### 3. Information We Process on Behalf of Customers

This Notice does not apply to clinical trial data we may process on behalf of our Customers, including any Personal Data of our Customers' clinical trial participants and relevant trial site staff ("Clinical Data") that ClinDART may necessarily process in the course of providing our Services to Customers.

#### **B. Our Role with Respect to Your Personal Data**

We do not always have the same degree of decision-making with respect to why and how each piece of Personal Data will be processed.

- Regarding the Personal Data of users of our business contacts and prospects of ClinDART, we decide the purposes and means of processing and consequently act as a data controller.

- Regarding Clinical Data, we do not decide *why* or *how* this will be processed, but our Customers do. Thus, we act as a data processor on behalf of our Customers in this context. We do not decide what Clinical Data is being stored, and we will only access the Clinical Data to provide the Services that our Customer has directed us to provide, or if we are required to do so by law. With regard to the processing of Clinical Data, the privacy notices of our Customers, rather than this Notice, will apply to the processing. If you have a direct relationship with one of our Customers, please contact them to exercise your privacy rights.

Please note that ClinDART's processing of Clinical Data only occurs after it has been pseudonymized, which means it has been stripped of all Personal Data that could reasonably be used to associate it to a data subject or identify a particular data subject as the source of that data. Additionally, ClinDART does not have access to the key to decrypt the pseudonymized data. The key is held by a separate third party, ensuring an extra layer of security. This means we cannot possibly determine what Clinical Data is yours at any time. Such circumstances mean that this data may not necessarily be considered Personal Data under certain data protection and privacy laws.

## **C. Collection of Personal Data and Purposes of Use**

### 1. Collection of Personal Data and Its Use

#### a. How and where does ClinDART collect Personal Data?

ClinDART collects Personal Data from data subjects who:

- i) Receive or send communications from/to us, including email, phone calls, and mail;
- ii) Use our Services as a Customer;
- iii) Submit a request for information;
- iv) Engage with our customer support services; or
- v) Work at a partner or supplier of ours and interact with ClinDART in the course of doing business or contemplating doing business with us.

#### b. From what sources do we typically collect Personal Data?

We collect Personal Data from you when you call, email, or otherwise interact with us.

What type of Personal Data do we typically collect?

For Customer contacts and Customer employees as well as business partners, we collect your contact information and the contents of your communications with us.

### 2. How We Use the Data

a. General Obligations

ClinDART collects Personal Data for a number of purposes, including but not only the following:

- i) Providing the Services, including:
  - Promoting the security of our and Services by tracking use, enforcing our terms and policies, investigating and preventing fraudulent, suspicious or illegal acts, and seeking to prevent any unauthorized access to the Services;
  - Operating and maintaining the Services (e.g., billing and account management);
  - Responding to inquiries for action, support and/or information;
  - Sending technical alerts, updates, or security notifications, plus educational and administrative communications.
- ii) Legitimate Interests:
  - Meeting contractual obligations to Customers and partners;
  - Enabling us to understand and engage with those interested in our Services, content, and work;
  - Analyzing Customers' use of the Services for trends, marketing, improvements, security purposes and continued proper functioning;
  - Sending updates and communications about us;
  - Conducting internal training and research.
- iii) Meeting Legal Obligations:
  - Working to meet legal obligations, limiting damages, complying with judicial proceedings, court orders or legal processes.

b. Otherwise, Where We Have Obtained Consent:

- i) We may disclose certain Personal Data to a third party with that person's consent.
- ii) Where we need to collect Personal Data by law or under a contract with you, and you fail to provide the Personal Data requested, such deficiency is likely to prevent us from meeting our obligations.
- iii) If you provide us with Personal Data relating to another person, you must confirm you have informed that other person of our identity and why their

Personal Data is required and how it will be used, and they must have given consent (written) to share their information with us. THEY have to consent and we will need evidence of that consent. Please know you cannot consent for them.

c. Sharing and Disclosure of Personal Data

We may share Personal Data to vetted and contract-bound third parties for certain business purposes, including the following:

- i) General Business Purposes: We may share information with consultants and service providers for Customer or technical support, marketing, recruiting, operations, security of our Services, account management, and legitimate business purposes;
- ii) Compliance with the Law: We may disclose information to a third-party where legally required to comply with applicable laws, regulations, legal processes or government requests;
- iii) Protection of our Rights: We may also disclose information where it is needed to protect, exercise, establish or defend our legal rights;
- iv) Business Transfers: We may share or transfer information to support negotiations of or for a merger, sale of company assets, financing, or acquisition of all or a portion of the ClinDART business to another company;
- v) Receiving Professional Advice: In certain instances, we may share Personal Data with professional advisers acting as processors, including lawyers, bankers, auditors and insurers, who provide professional services, but only to the extent we legally must do so or have a legitimate interest in sharing information.

## D. Lawful Bases for Processing

To use your Personal Data, we must have a valid reason, which under some laws is called the “lawful basis for processing” or “legal grounds for processing.” We may process your Personal Data based on these reasons:

- Your Consent: Sometimes, we will use your Personal Data because you actively indicated it is okay that we do so. This includes, for example, your consent for us to contact you for marketing purposes.
- Legitimate Interests: This includes using your Personal Data to fulfill our agreement with you by, for example, providing you with the Services.
- Following the Law: This includes processing your Personal Data to follow the law, such as keeping records of your cookie choices to comply with EU law, such as the e-Privacy Directive and the General Data Protection Regulation.

- Other Reasons: This includes using your Personal Data for any other reason that the law allows.

When we use your Personal Data because you gave us permission (consent), you can change your mind at any time. However, this will not undo the things we did with your data before you changed your mind. It also will not change the things we are allowed to do with your data based on other reasons.

## **E. International Transfers, Security, and Data Retention**

### **1. International Transfers of Your Personal Data: Europe**

When your Personal Data is safeguarded by the EU or UK General Data Protection Regulation, or Swiss data protection law, before sending it to parties outside of the European Economic Area (“EEA”), the UK, or Switzerland, we will do one of two things:

- Seek your consent; or
- Demand privacy and security: We will ensure the third party maintains the same level of privacy and security for your Personal Data as we do.

In some cases, the authorities of a country may have determined that the laws of other countries, territories or sectors within a country provide a level of protection equivalent to domestic law. You can see [here](#) the list of countries, territories and specified sectors that the European Commission recognized as providing an adequate level of protection for Personal Data, [here](#) the list of the UK, and [here](#) the list of Switzerland.

We are accountable for the protection of your Personal Data when we transfer it to others. We either send it to a country, territory or sector within a country that is recognized as providing the same level of Personal Data protection as the country of origin, or use safeguards like the [Standard Contractual Clauses](#) (also known as the “SCCs”) approved by the European Commission under [Article 46.2 of the GDPR](#), with necessary adjustments for transfers from the UK or Switzerland, or use specific transfer instruments like the [UK International Data Transfer Agreement](#).

### **2. Security**

We are strongly committed to keeping your Personal Data safe. We have implemented and will maintain technical, administrative, and physical measures that are reasonably designed to help protect your Personal Data from unauthorized processing. Unauthorized processing includes unauthorized access, exfiltration, theft, disclosure, alteration, or destruction. Some of these measures include encryption, and we have dedicated teams responsible for information security and privacy.

### **3. Data Retention**

We retain your Personal Data for as long as needed for the purpose we collected it and any other permitted linked purpose and in accordance with our data retention policies. For example, 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. If we use your data for multiple purposes, we keep it until the purpose with the longest retention period expires, discontinuing use for shorter periods. Our retention periods align with our business needs and industry standards.

#### 4. Right to Lodge a Complaint with a Supervisory Authority

If the EU or UK General Data Protection Regulation applies to our processing of your Personal Data, you have the right to lodge a complaint with a supervisory authority if you are not satisfied with how we process your Personal Data.

Specifically, you can lodge a complaint in the Member State of the European Union of your habitual residence, place of work, or the alleged violation of the GDPR. In the UK, you can lodge a complaint with the UK Information Commissioner's Office.

#### F. Cookies

A “cookie” is a small file stored on your device when you visit a website or application that contains information about your device. We do not use any cookies on our website, and as such, we do not collect or process any Personal Data or any other kind of information from our website visitors.

#### G. Your Privacy Rights

##### 1. What You Can Ask Us to Do

You have specific rights regarding your Personal Data that we collect and process. Please note that you can only exercise these rights with respect to Personal Data that we process about you when we act as a data controller.

Our processing of your Personal Data on behalf of one of our Customers is outside the scope of this Notice. To exercise your rights with respect to this Personal Data, please read the privacy notice of that Customer.

You can access, update, change, request a machine-readable copy of (portability) or delete Personal Data we may have with regard to your interaction with us directly where we act as a data controller, which is when you directly provide your Personal Data to us. You also have the right to ask us to restrict the processing of your Personal Data and to object to the processing of your Personal Data. You can withdraw your consent for the processing of your data at any time. Please note if you withdraw your consent, our use of your Personal Data before you withdraw your consent is still lawful.

If you wish to exercise your rights related to Personal Data where you are or were a clinical trial participant, and we are the data processor, you must do so by contacting your clinical trial sponsor company. You may also contact us via email at [info@clindart.com](mailto:info@clindart.com) or by using the contact details provided under the “[Contact Us](#)” heading below. If the clinical trial sponsor you name in your request is a current or former Customer of ClinDART, we will redirect your request to the clinical trial company you name in your request. NOTE: As explained above in this Privacy Notice, ClinDART cannot identify your Clinical Data from our end. If you do not or cannot identify the clinical trial company you provided your data to, we cannot relay your request.

**For a Personal Data request, please contact us using one of the methods described in the [Contact Us](#) section below and provide the following:**

- a. your name;
- b. type of request;
- c. the name of your clinical trial sponsor company (if applicable);
- d. approximate date of collection of the information; and
- e. a valid email address to contact you.

ClinDART does not use or process any Personal Data which would subject a person to a decision based solely on automated processing, including profiling, which produces legal effects (“Automated Decision-Making”). Automated Decision-Making currently does not take place on our website(s) or in or as part of our Services.

You have the right to opt-out of marketing communications we send at any time. You can exercise this right by clicking the “unsubscribe” link in the marketing communications or by using the contact details provided under the “[Contact Us](#)” heading below. Please note opting out of the receipt of marketing communications from us does not opt you out of receiving important business communications related to your current relationship with us, such as communications related to service announcements or security information, service announcements or security information.

If we have collected and used your Personal Data with your consent, you can withdraw your consent. Withdrawing your consent will not affect the lawfulness of any processing conducted prior to that withdrawal, nor will it affect the use conducted in reliance on lawful processing grounds other than consent.

## 2. Verification of a Consumer Request

Please note we may need to verify your identity in connection with your requests, and such verification process may, if you do not have access to your account, require you to provide additional information maintained about you to verify your identity. We may request additional information if believed necessary to verify your identity. If we are unable to verify your identity or request, we may not, in accordance with applicable law, be able to fulfill your request.

## 3. Response Timing and Format

We will promptly confirm receipt of your request, and we will substantively respond to a verifiable consumer request as soon as possible but within one month of its receipt. If we need more time (up to another two months), we will inform you of the reason and extension period in writing within one month of receiving your initial request.

We will not charge a fee to process or respond to a verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine the request warrants a fee, we will tell you why that decision was made and provide you with a cost estimate before completing your request.

## 4. The Global Privacy Control and Do Not Track Signal

We do not utilize or allow cross-contextual behavioral advertising (“ad tracking”) technologies. As such, our website(s) does not recognize the Global Privacy Control (“GPC”) signal as no technologies are deployed by us requiring that type of blocking. Regardless, note that the GPC is a browser setting allowing consumers to opt-out of targeted advertisements and/or the sale of Personal Data through a pre-determined signal. The GPC signal allows you to make a single opt-out request that applies to websites that are able to recognize the signal.

## **H. Children**

Our Services and website(s) are not geared or in any way directed to data subjects under the age of 18. We do not knowingly collect Personal Data from those under 18. If you are a parent or guardian and believe your child has provided Personal Data to us without your consent, please send an email to [info@clindart.com](mailto:info@clindart.com), or reach out by any method identified in the [Contact Us](#) section below, and we will take steps needed to delete any under 18 Personal Data from our systems.

## **I. Changes to Our Privacy Notice**

We regularly review and update this Notice. Your continued use of our website(s) and Services following posted changes constitutes notice and acceptance of such changes. If you do not accept the new changes, please do not use our website(s) and Services.

## **J. Contact Us**

If you have questions or comments about this Notice, the ways ClinDART collects and uses Personal Data, your choices and rights regarding that use, or you wish to exercise your rights under applicable data privacy laws, please do not hesitate to contact us at:

Email: [info@clindart.com](mailto:info@clindart.com)

Postal Address:

ClinDART, Inc.  
Attn: Privacy Team  
16935 W Bernardo Dr Ste 103  
San Diego, CA 92127

Please allow up to four weeks for us to reply. If you need to access this Notice in an alternative format due to having a disability, please contact [info@clindart.com](mailto:info@clindart.com).

### **1. European Union Representative**

We have appointed [VeraSafe](#) as our representative in the EU for data protection matters. While you may also [contact us](#), VeraSafe can be contacted on matters related to the processing of Personal Data. To contact VeraSafe, please use this contact form: <https://www.verasafe.com/privacy-services/contact-article-27-representative/> or via telephone at: [+420 228 881 031](tel:+420228881031)

Alternatively, VeraSafe can be contacted at:

**VeraSafe Ireland Ltd**  
Unit 3D North Point House  
North Point Business Park  
New Mallow Road  
Cork T23AT2P  
Ireland

2. United Kingdom Representative

We have appointed [VeraSafe](#) as our representative in the UK for data protection matters. While you may also [contact us](#), VeraSafe can be contacted on matters related to the processing of Personal Data. To contact VeraSafe, please use this contact form: <https://www.verasafe.com/privacy-services/contact-article-27-representative/> or via telephone at: +44 (20) 4532 2003.

**VeraSafe United Kingdom Ltd.**

37 Albert Embankment  
London  
SE1 7TL  
United Kingdom

3. Data Protection Officer

We have appointed [VeraSafe](#) as our Data Protection Officer (“DPO”). While you may contact us directly, VeraSafe can also be contacted on matters related to the processing of Personal Data. VeraSafe’s contact details are:

**VeraSafe LLC**  
100 M Street S.E., Suite 600  
Washington, D.C.  
20003  
USA

Email: [experts@verasafe.com](mailto:experts@verasafe.com)  
Web: <https://www.verasafe.com/about-verasafe/contact-us/>