Datacubed Health
Privacy Policy
Effective Date: 1 April 2022

Introduction
Your privacy matters to us at Datacubed Health. This Privacy Policy (Policy) explains how we may collect, use, and share personal information. It applies to our website, services, information, tools, functionality, updates, and similar materials (collectively Services). You have several rights concerning your information. Please read the Policy carefully to understand what we do and what your rights are.

Incorporated Terms
The following additional terms are incorporated into this Policy as if fully set forth herein:

- End User Terms of Service
- Children's Privacy Policy
- Cookie Policy

Who we are
We are Data Cubed, LLC d/b/a Datacubed Health. We can be reached at legal@datacubed.com and at:

Datacubed Health
384 Bridge Street
4th Floor
Brooklyn, NY 11201

Datacubed Health is a pioneering technology company making better science and healthier communities a reality. We apply individualised solutions for the capture of data, including smartphone apps, wearable, in-home, and environmental sensors, for remote engagement with patients and for virtual clinical studies. In connection with the research, trials, studies, patient-engagement initiatives, or projects that we conduct on behalf of companies and heath care organisations ("Clinical Research Studies") and educational institutions ("Academic Studies") (collectively "Studies"), we sometimes collect information from you.

References to "we," "us" and "our" mean Datacubed Health. References to "third-party" mean someone who is not you or us.

We are a Processor of the personal information Client Participants provide to us. We are a Controller of the personal information Datacubed Health Participants provide to us.

Who you are

In the Policy, "you" means you as a:

- Client – an employee or a representative of a business that uses Datacubed Health
- Client Participant – an individual solicited by a business who participates in a study conducted by Datacubed Health on behalf of the business
- Datacubed Health Participant – an individual who participates in a study conducted by Datacubed Health on its own behalf

You as a Client are a Controller of the Client Participant personal information you provide to us.

What legal basis we have for processing personal information

We process your personal information based on:

- Consent you provide to us or to our Client in connection with the Studies that we conduct. You have the right to withdraw your consent at any time. You can withdraw your consent for us processing your personal information by contacting us at legal@datacubed.com or for contacting our Client, the sponsor of the Study, via the clinical site where the study is being carried out. The processing conducted in connection with the Studies under the legal ground of "Consent" is:
    - The collection of personal information from Client Participants and Datacubed Health Participants, and
    - The collection and use of personal information to provide the Services.
- To the extent not outweighed by your rights under applicable law, our Legitimate Business Interests. The processing conducted under the legal ground of "Legitimate Business Interests" is to:
    - Respond to service and technical support issues and requests,
    - Fulfil your requests made to our website and helpdesk or sent to legal@datacubed.com
    - Develop and improve the Services

What personal information we collect

As a Client Participant or a Datacubed Health Participant in an Academic Study, we may collect the following information when you sign up to participate, and participate, in an Academic Study:

- Name
- Address
- Date of birth
- Place of birth
- Email address
- Username
- Information from your activities and devices used on the Services

- Location for use with Geofencing features, as applicable
- Phone device information
- Bluetooth device information
- Phone contacts
- Cell metadata
- SMS message metadata
- IP addresses
- Social media metadata
- Demographic information (ethnicity, gender, height, and weight)
- Medical condition
- Medical dosage and/or dosage change details
- Medical injection site and injection date details
- Survey information for Health, Economics and Outcomes Research (HEOR) data

As a Client Participant or a Datacubed Health Participant in a Clinical Research Study, we may collect the following information when you sign up to participate, and participate, in a Clinical Research Study:

- First Name, and optionally surname
- Email address
- Information from your activities and devices used on the Services
- Location for use with Geofencing features, as applicable
- IP addresses
- Medical condition
- Medical dosage and/or dosage change details
- Medical injection site and injection date details
- Survey information for Health, Economics and Outcomes Research (HEOR) data

As a Client, we may collect the following information:

- Name
- Business address
- Business telephone number
- Business email address
- Any messages you send us
- Billing information
- Other details necessary to provide our services to you

As the Client, you are the Controller of this information, and we are a Processor of this information.

How we may use personal information

We use the information we collect from you as a Client Participant or a Datacubed Health Participant to provide the Services to you. We may also use this information to help us develop and improve our Services, fulfil your requests, and for other purposes permitted by law.

If you are a Client Participant, our processing of your information is restricted to what is agreed to in a contract with the Client. We only share pseudonymised data with the Client, the sponsor of the Study.

We use the information we collect from Clients to answer your inquiries and to provide the Services to you.

How we may share personal information

We share personal information with our service providers on a confidential basis in order for them to provide services to us, to you, and to enable us to provide the Services:

- Amazon Web Services, Inc. (AWS) provides servers in the United States (U.S.) and Germany that store all personal information collected from you
- The Rocket Science Group LLC d/b/a Mailchimp, located in the U.S., helps us manage email communications
- Stefanini Group, located in the U.S., Belgium, Romania, China, Poland, and the Philippines, helps us manage support tickets
- Twilio, Inc., located in Germany and the U.S., helps us send and receive text messages and provides video conferencing
- Splunk, Inc., located in Germany and the U.S., and Sisense, Ltd., located in Germany and the U.S., helps us analyse and provide performance reports about the personal information

At the direction of our Clients, we share personal information with hospitals and clinics who provide services on behalf of our Clients.

We may share personal information with government and/or law enforcement agencies to the extent we believe it necessary to comply with the law, such as in response to a subpoena or court order, to defend a legal claim or establish or protect our legal rights or otherwise as permitted by applicable law. We commit to reviewing the legality of any subpoena or court order to disclose data, to challenging the subpoena or court order if, after a careful assessment, we conclude that there are grounds to do so, to seeking interim measures to suspend the effects of the subpoena or court order until the court has decided on the merits, to not disclosing the personal data requested until required to do so under the applicable procedural rules, and to providing the minimum amount of information permissible when responding to the subpoena or court order, based on a reasonable interpretation of the subpoena or court order. The information shared depends on what is sought by the subpoena or court order.

We may disclose personal information in our possession in the event we believe it necessary or appropriate to prevent criminal activity, personal injury, property damage or bodily harm. The personal information disclosed depends on the circumstances.

We may transfer your information to a successor in interest, which may include but may not be limited to a third party in the event of an acquisition, sale, asset sale, merger, or bankruptcy. The policies applicable to your information thereafter may be determined by the transferee, unless otherwise prohibited by law. The personal information transferred would consist of the personal information collected as described above.

Any third party with whom we share your information will provide the same or equal protection of your information as stated in the Policy and as required by the Apple App Guidelines.

Where we store and process personal data

We store the information we collect from you on servers provided by AWS in the U.S. and the European Union (EU). For testing purposes, the information we collect from you may also be stored on desktop and laptop computers used by our employees in the U.S. The information we collect from you in the European Economic Area (EEA), the United Kingdom (UK), and Switzerland may be transferred from and kept outside the EEA, the UK, and Switzerland because our operations and some of our servers are located in the U.S. We enter into Standard Contractual Clauses in order to transfer your information outside the EEA, the UK, and Switzerland. We have withdrawn from the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the EEA and Switzerland to the U.S.; we will continue to apply the Privacy Shield Principles to personal information that we received while participating in the Privacy Shield Frameworks. To learn more about the Privacy Shield programme, visit https:// www.privacyshield.gov/.

How long we may keep your personal data

We may keep your information for as long as we have to by law. If there is no contradictory legal requirement, we will only keep it for as long as we need it to perform the Services. We may also keep your information for a reasonable period of time. For example, where U.S. law applies, and where required by U.S. law, we retain covered protected health information for 7.5 years or as otherwise required or permitted by law, and where the International Conference on Harmonisation Guidelines for Industry Structure and Content of Clinical Study Reports apply, Clinical Research Study data are retained for a period of 25 years as of completion of the Services or longer as required by local law.

.

Where to find us on social media and Cookies

You can find us on Facebook, Twitter, and LinkedIn. When you visit our social media pages, you can control the settings of cookies that are not essential to provide the services you request. A cookie is a small file placed on your device that enables features and functionality of the

www.datacubed.com website. The Datacubed Health Cookie Policy explains what cookies are, our use of cookies, and how you can manage cookies. Except for those cookies that are essential for the Service that you have requested, no cookie will remain on your device, and we will not retain any information collected from cookies, longer than is permitted by law.

Your rights regarding your information

You have the right:

- To know if we are collecting, using, or sharing your information and to request access to this information
- To request that we correct your information if it is inaccurate or incomplete
- To ask us to erase your information if
    - Your information is no longer necessary for the purposes for which it was collected, used, or shared
    - You withdraw the consent on which the collection, use, or sharing is based
    - You object to the collection, use, or sharing and there is no overriding legitimate interest for continuing the collection, use, or sharing
    - You object to the collection, use, or sharing of your information for direct marketing purposes
    - Your information was unlawfully collected, used, or shared
    - Your information has to be erased in order to comply with a legal obligation
    - Your information was collected in order to offer online services to children
- To obtain from us a restriction on the collection, use, or sharing of your information if
    - You contest the accuracy of your information
    - You have objected to the collection, use, or sharing based on legitimate interest and we are considering whether our or a third party's legitimate interest ground overrides your interest
    - The collection, use, or sharing is unlawful, and you oppose erasure and request that use be restricted instead
    - We no longer need your information, but you require your information to establish, exercise, or defend a legal claim
- To be able to take with you the information you provided to us and to transmit that information to another organisation where our collection, use, or sharing of that information is carried out by automated means and is based on your consent or the performance of a contract
- To object to collection, use, or sharing based on the purposes of legitimate interest or performance of a legal task, direct marketing, and scientific/historical research and statistics
- 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
- To lodge a complaint with a supervisory authority

How you exercise your rights

You may access, correct, or delete your account information or cancel your account at any time by emailing us at legal@datacubed.com. Please note that in some cases we may retain certain information about you as required by law.

Governing law

EU laws govern the Policy.

Changes to the Policy

The Policy is current as of the Effective Date set forth above. We may change the Policy from time to time, so be sure to check back periodically. We will post any changes to the Policy on our site at www.datacubed.com.