

COVID-19 Symptom Tracker App Privacy Policy US

Effective Date: March 27, 2020

At Zoe Global Limited (together with its affiliates, “Zoe,” “we,” “us”) we take your privacy seriously. Please read the following to learn how we treat your personal information. By using or accessing the COVID-19 Symptom Tracker app and associated website covid.joinzoe.com (together, the “Services”) in any manner, you acknowledge that you accept the practices and policies outlined in this Privacy Policy, and you hereby consent that we will collect, use, and share your information in the following ways.

Remember that your use of our Services is at all times subject to our [Terms of Use](#), which incorporates this Privacy Policy. Any terms we use in this Policy without defining them have the definitions given to them in the Terms of Use.

What this Privacy Policy Covers

This Privacy Policy covers how we treat Personal Data that we gather when you access or use our Services. “Personal Data” means any information that identifies or relates to a particular individual and also includes information referred to as “personally identifiable information” or “personal information” under applicable data privacy laws, rules, or regulations.

Sources of Personal Data

We collect Personal Data about you from:

- You:
 - when you provide such information directly to us, and
 - when Personal Data about you is automatically collected in connection with your use of our Services.
- On our COVID-19 Tracker website <https://covid.joinzoe.com/us> we collect Personal Data through cookies and similar technologies such as pixel tags, web beacons, clear GIFs, and JavaScript (collectively, “Cookies”) to enable our servers to recognize your web browser and tell us how and when you visit and use our website, to analyze trends, learn about our user base and operate and improve our website. Cookies are small pieces of data— usually text files – placed on your computer, tablet, phone, or similar device when you use that device to visit our Services. We may also supplement the information we collect from you with information received from third parties, including third parties that have placed their own Cookies on your device(s). For example, Google, Inc. (“Google”) uses cookies in connection with its Google Analytics services. Google’s ability to use and share information collected by Google Analytics about your visits to the Services is subject to the Google Analytics Terms of Use and the Google Privacy Policy. You have the option to opt-out of Google’s use of cookies by visiting the Google advertising opt-out page at www.google.com/privacy_ads.html or the Google Analytics Opt-out Browser Add-on at <https://tools.google.com/dlpage/gaoptout/>. Please note that because of our

use of Cookies, the website does not support “Do Not Track” requests sent from a browser at this time. For more information about our use of cookies, please see our [Cookie Policy](#)

Personal Data We Collect

We collect and process of the following types of Personal Data about you:

Personal Identifiers:

We collect personal identifiers from you and your device such as your name (optional), email address (optional), phone number (optional), a user name and password, IP address, device ID, location (zip code) and other identifiers including your year of birth. Note that providing your name and phone number is optional. We also collect your IP address (All of the foregoing, “Personal Identifiers.”)

We process Personal Identifiers for the purposes of providing you the Services and developing, improving, promoting and running the Services. For example, we share some of these personal identifiers with medical researchers at Harvard T Chan School of Public Health, Massachusetts General Hospital, King's College London and Stanford University School of Medicine. We may ask for your feedback on the app and we may conduct other surveys (which are of course voluntary). We may also send you information about new versions of the app or similar apps we may have in the future. Every marketing email sent by us will include a link you can click to opt-out from receiving such emails.

Health data and other protected classification characteristics:

Through our Service, you may choose to submit health related information about yourself, such as your sex at birth and how you identify today, your age, your height, weight and information about your health, pre-existing conditions and symptoms (including your body temperature). You may also submit your COVID-19 test status and details of any treatment, whether you are a healthcare worker and your use of protective equipment, and visits to hospital or clinics. (All of the foregoing, “Health Data and Other Protected Classifications”)

We process Health Data and Other Protected Classifications for the following purposes:

- To better understand symptoms of COVID-19
- To track the spread of COVID-19
- To advance scientific research into the links between patient's health and their response to infection by COVID-19
- To identify the exposure of healthcare workers to COVID-19
- To provide you with the Services
- In the future we may use this data to help healthcare providers such as hospitals support sick individuals

Personal Data of Children

As noted in the Terms of Use, we do not knowingly collect or solicit Personal Data from children under 18; if you are a child under 18, please do not attempt to register for or otherwise use the Services or send us any Personal Data. If we learn we have collected Personal Data from a child under 18, we will delete that information as quickly as possible. If you believe that a child under 18 may have provided us Personal Data, please contact us at dpo@joinzoe.com.

Sharing of Personal Data

Third party processors: We use third parties to process some of your Personal Data on our behalf, for example security and fraud prevention providers, hosting and other technology and communications providers, analytics providers, and staff augmentation and contract personnel. When we allow them access to your data, we do not permit them to use it for their own purposes. We have in place with each processor a contract that requires them only to process the data on our instructions and to take proper care in using it.

These processors include:

- Amazon Web Services
- Google Cloud Platform
- SurveyMonkey
- Segment
- Google Analytics
- Mixpanel
- Google G Suite
- MailChimp
- Mailgun
- Intercom
- Sentry
- Google Firebase
- SwiftyBeaver

Research Partners and Other Third Parties:

Research Partners: The purpose of our Services is to understand and prevent the spread of COVID-19. In order to do this, we share data with people doing health research, for example, people working in:

- Hospitals
- Clinics
- Universities
- Health charities
- Other research institutions

For example, doctors and scientists at Massachusetts General Hospital, Harvard School of Public Health, Stanford University, and King's College London will have access to your Personal Data for the foregoing purpose. Below is a list of institutions with whom we share your Personal Data. (Please note that this list is provided as an example only, and we may

add institutions to this list.) Data shared with research partners other than hospitals and teaching institutions will be de-identified.

Institutions we share data with include (without limitation):

Harvard University
Stanford University
Massachusetts General Hospital
Tufts University
Berkeley University
King's College London
Guys & St Thomas' Hospitals
UK National Health Service
Nottingham University
University of Trento
Lund University

Transfer: We may restructure how we provide the Services, and as part of that, your Personal Data may be transferred to one of our affiliates or to a not-for-profit organization.

Data Security and Retention

We seek to protect your Personal Data from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of Personal Data and how we are processing that data. Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the Internet or storing data is completely secure. We cannot guarantee the complete security of any data you share with us, and except as expressly required by law, we are not responsible for the theft, destruction, loss or inadvertent disclosure of your information or content.

We are unable today to set any particular time limit on the storage of your sensitive personal data, but we will keep it under regular review and ensure that it is not kept longer than is necessary. By way of example, we currently collect your name so that we are able to pass this on to health care professionals if it is necessary to protect your vital interests or the vital interests of another person. Once this is no longer required, we will delete all names from our records. In contrast, data about the spread of the virus is likely to be extremely valuable for researchers studying both this virus and in understanding epidemic spread for the future. We are likely, therefore, to retain this information for much longer

In some cases we retain Personal Data for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or is otherwise required by applicable law, rule or regulation. We may further retain information in an anonymous or aggregated form where that information would not identify you personally.

Your rights

California Resident Rights

California privacy law requires us to provide the following information, even though we do not sell your data:

If you are a California resident, you have the rights outlined in this section under the California Consumer Privacy Act (“CCPA”). Please see the “Exercising Your Rights” section below for instructions regarding how to exercise these rights. If there are any conflicts between this section and any other provision of this Privacy Policy and you are a California resident, the portion that is more protective of Personal Data shall control to the extent of such conflict. If you have any questions about this section or whether any of the following applies to you, please contact us at

Access

You have the right to request certain information about our collection and use of your Personal Data over the past 12 months. We will provide you with the following information:

- The categories of Personal Data that we have collected about you.
- The categories of sources from which that Personal Data was collected.
- The business or commercial purpose for collecting or selling your Personal Data.
- The categories of third parties with whom we have shared your Personal Data.
- The specific pieces of Personal Data that we have collected about you.

If we have disclosed your Personal Data for a business purpose over the past 12 months, we will identify the categories of Personal Data shared with each category of third party recipient.

Deletion

You have the right to request that we delete the Personal Data that we have collected from you.

Exercising Your Rights

To exercise the rights described above, you must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected Personal Data, and (2) describes your request in sufficient detail to allow us to understand, evaluate, and respond to it. Each request that meets both of these criteria will be considered a “Valid Request.” We may not respond to requests that do not meet these criteria. We will only use Personal Data provided in a Valid Request to verify you and complete your request. You do not need an account to submit a Valid Request.

We will work to respond to your Valid Request within 45 days of receipt. We will not charge you a fee for making a Valid Request unless your Valid Request(s) is excessive, repetitive, or manifestly unfounded. If we determine that your Valid Request warrants a fee, we will notify you of the fee and explain that decision before completing your request.

You may submit a Valid Request using the following methods:

Email us at: dpo@joinzoe.com

Personal Data Sales

We do not sell your Personal Data.

We Will Not Discriminate Against You for Exercising Your Rights Under the CCPA

We will not discriminate against you for exercising your rights under the CCPA.

Other State Law Privacy Rights

California Resident Rights

We will not provide your Personal Data to third parties for such third parties' direct marketing purposes;

Your browser may offer you a "Do Not Track" option, which allows you to signal to operators of websites and web applications and services that you do not wish such operators to track certain of your online activities over time and across different websites. Our Services do not support DO Not Track requests at this time. To find out more about "Do Not Track," you can visit www.allaboutdnt.com.

Nevada Resident Rights

Nevada law requires the following wording even though we do not sell your data: If you are a resident of Nevada, you have the right to opt-out of the sale of certain Personal Data to third parties who intend to license or sell that Personal Data. You can exercise this right by contacting us at dpo@joinzoe.com with the subject line "Nevada Do Not Sell Request" and providing us with your name. We do not sell your Personal Data as defined in Nevada Revised Statutes Chapter 603A.

European Union Data Subject Rights

EU Residents

You may have additional rights under the EU General Data Protection Regulation (the "GDPR") with respect to your Personal Data, as outlined below.

For this section, we use the terms "Personal Data" and "processing" as they are defined in the GDPR, but "Personal Data" generally means information relating to an identifiable person, and "processing" generally covers actions that can be performed in connection with data such as collection, use, storage and disclosure. Zoe Global Limited will be the controller of your Personal Data processed in connection with the Services.

If there are any conflicts between this this section and any other provision of this Privacy Policy, the policy or portion that is more protective of Personal Data shall control to the

extent of such conflict. If you have any questions about this section or whether any of the following applies to you, please contact us at dpo@joinzoe.com.

Personal Data Use and Processing Grounds

We will only process your Personal Data if we have a lawful basis for doing so. Lawful bases for processing include consent and our “legitimate interests” or the legitimate interest of others, as further described below.

Legitimate Interests: Our legal basis for processing your Personal Identifiers is our legitimate interest in providing you the Services and developing, improving, marketing and running the Services.

Consent: In some cases, we process Personal Data based on the consent you expressly grant to us at the time we collect such data. When we process Personal Data based on your consent, it will be expressly indicated to you at the point and time of collection. Specifically, we process the category of Health Data and Other Protected Classifications based on your consent. Because of the tight regulatory requirements placed on us, we need your consent to process data about your health, which means that if you do not consent (or withdraw your consent), we cannot allow you to use the app. This is not meant unkindly, we are simply not able to provide you with the service without your consent.

If you wish us to stop processing Health Data and Other Protected Classifications, you may withdraw your consent at any time by emailing us at leavecovidtracking-us@joinzoe.com. When you withdraw your consent, we will delete all Health Data and Other Protected Classifications we hold about you.

Other Processing Grounds: From time to time we may also need to process Personal Data to comply with a legal obligation, if it is necessary to protect the vital interests of you or other data subjects, or if it is necessary for a task carried out in the public interest.

EU Data Subject Rights

Under the [GDPR](#) you have a number of important rights with respect to your Personal Data, including those set forth below. For more information about these rights, or to submit a request, please email us at dpo@joinzoe.com. Please note that in some circumstances, we may not be able to fully comply with your request, such as if it is frivolous or extremely impractical, if it jeopardizes the rights of others, or if it is not required by law, but in those circumstances, we will still respond to notify you of such a decision. In some cases, we may also need to you to provide us with additional information, which may include Personal Data, if necessary to verify your identity and the nature of your request.

- **Access:** You can request more information about the Personal Data we hold about you and request a copy of such Personal Data. You can also access certain of your Personal Data by logging on to your account.
- **Rectification:** If you believe that any Personal Data we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data.

- **Erasure:** You can request that we erase some or all of your Personal Data from our systems.
- **Withdrawal of Consent:** If we are processing your Personal Data based on your consent (as indicated at the time of collection of such data), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, you may have to then provide express consent on a case-by-case basis for the use or disclosure of certain of your Personal Data, if such use or disclosure is necessary to enable you to utilize some or all of our Services.
- **Portability:** You can ask for a copy of your Personal Data in a machine-readable format. You can also request that we transmit the data to another controller where technically feasible.
- **Objection:** You can contact us to let us know that you object to the further use or disclosure of your Personal Data for certain purposes, such as for direct marketing purposes.
- **Restriction of Processing:** You can ask us to restrict further processing of your Personal Data.

For further information on each of those rights, including the circumstances in which they apply, see the [Guidance from the United Kingdom Information Commissioner's Office \(ICO\) on individuals rights under the General Data Protection Regulation](#).

If you would like to exercise any of those rights, please email, call or write to our data protection officer using the contact details given below.

The [General Data Protection Regulation](#) also gives you the right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/make-a-complaint/your-personal-information-concerns/> or telephone: +44 0303 123 1113.

Transfers of Personal Data

The Services are hosted and operated in the United Kingdom and in the United States ("U.S.") through Zoe Global Limited and its service providers and the third parties with whom we share information (see the **Sharing of Personal Data** section above), and laws in the U.S. may differ from the laws where you reside. By using the Services, you acknowledge and agree that any Personal Data about you, regardless of whether provided by you or obtained from a third party, is being provided to Zoe Global Limited and third parties (as disclosed in this Privacy Policy) in the U.S. and will be hosted on U.S. servers, and you authorize Zoe to transfer, store and process your information to and in the U.S., and possibly other countries.

Changes to this Privacy Policy

We're constantly trying to improve our Services, so we may need to change this Privacy Policy from time to time as well, but we will alert you to changes by placing a notice in the

app or on our website, by sending you an email, and/or by some other means. Please note that if you've opted not to receive legal notice emails from us (or you haven't provided us with your email address), those legal notices will still govern your use of the Services, and you are still responsible for reading and understanding them. If you use the Services after any changes to the Privacy Policy have been posted, that means you agree to all of the changes. Use of information we collect is subject to the Privacy Policy in effect at the time such information is collected.

About us

Our address is: Zoe Global Limited, 164 Westminster Bridge Road, London SE1 7RW, United Kingdom

Data Protection Officer: dpo@joinzoe.com
