# Privacy Notice

All previous privacy notices and current and previous consents can be found here.

This page explains how we process information about individual people, known as “personal data”, that we collect through our COVID monitoring app. If you are using the app and entering your own personal data, then this applies to you. We may also be processing your personal data if someone else – a family member or parent or guardian or member of your household – has entered it on your behalf, see the section headed “recording information for others” for more information about this.

We process two kinds of information about you:

## Sensitive personal data

This is information about you, your health and your symptoms if unwell. It includes:

- Information about your health (including your height and weight) and any pre-existing conditions you may have.
- Information about any symptoms you may have (including body temperature).
- Your COVID-19 test status.
- Details of any treatment you have received for COVID.
- General information about you such as your sex at birth, your year of birth and your address.
- Whether you are a health worker coming into contact with patients.
- Whether you are a member of the UK twins study.
- Whether you have received a COVID-19 vaccine and supporting information relating to your vaccine (including dose dates, type of vaccine, batch number etc.)
- Information about any adverse effects you may experience after a COVID-19 vaccine.

We may also ask other questions from time to time, such as:

- Information about your diet.
- Information about your mental health.
- What you do if and when you go out, such as where you go and whether you wear a mask or other protection.
- Your feelings about receiving a COVID-19 vaccine.

We process this data in order that:

- We can better identify and understand symptoms of COVID-19.
- We can follow the spread of COVID-19, for example so that we can identify hotspots.
- We can provide an early detection system for diseases such as COVID-19 (or new variants of it)
- We can identify the exposure of healthcare workers to COVID-19.
- We can advance scientific research into the links between patients' health and their response to infection by COVID-19.
- We can track the uptake of COVID-19 vaccines and advance scientific research into the impact and effects of vaccination programmes.
- More generally, in helping to combat the spread of COVID-19 and improve the treatment and prophylaxis of it (including via patient identification for treatment and vaccine trials).

Our legal basis for processing it is that you consented to our doing so. 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.

We share this data with people doing health research, for example, people working in:

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

A full list of institutions we have shared data with can be found at the bottom of this page. An anonymous code is used to replace your personal details when we share this with researchers outside the NHS or King's College London.

Before sharing any of your data with researchers outside of the UK, we will remove your name, phone number, email address and the last 3 digits of your post code to protect your privacy.

Because of the nature of the research we carry out, we are unable 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.

If you wish us to stop processing your sensitive personal data, you may withdraw your consent at any time by emailing us at leavecovidtracking@joinzoe.com. When you withdraw your consent, we will delete all sensitive personal data we hold about you.

## Other personal data

We also collect contact information and other information from your device including:

- your name (optional)
- email address (optional)
- phone number (optional)
- a user name and password
- IP address
- device ID

We may use your email address, in order to send you emails for the following purposes:

- Sending you regular updates about the progress of the study from Professor Tim Spector of King’s College London.
- Occasionally, providing you with information regarding COVID-19 research and/or research articles.
- Occasionally, inviting you to participate in further COVID-19 research studies.
- Offering you the opportunity to take a COVID-19 test (for example if you have said you were unwell).

- Fundraising to support the COVID-19 symptom study or the COVID-19 related health research.
- Asking you for feedback on the app or conducting other forms of survey.
- Keeping in touch with you about the app and its performance as well as about new versions of the app or similar apps we may develop.

If you do not wish to receive emails from us regarding this information, then you can opt out by clicking the opt out link contained in our email. We do not sell your contact information to third parties.

As well as your email, we use this information for:

- Improving your user experience through the use of cookies.
- Identifying faults or other problems connected with the app.

Our legal basis for processing this information is our legitimate interest in developing, marketing and running the app and providing you with information as part of your experience of using the app.

We keep your contact information for 6 years after the last communication with us, or the last use of the app, for liability purposes, then we delete it.

## Cookies

Our use of cookies is a little more complicated, so we have written a detailed Cookie Policy, explaining what cookies are and explaining in detail how we process different kinds of cookies.

## Recording information for others

The app also allows users to input information about other people in addition to their own by making a separate profile for them. If you do this and the other person is able to understand the concept of consent, for example if they are a mentally competent adult or mature child, then you must only do this if they have given their consent.

Younger children may not be mature enough to give consent, but they may be able to understand what you are doing. If so, you should explain to them what you are doing and what may happen to information about them to the extent they are capable of understanding. You should also try to take into account their views, even if you make the ultimate decision. We trust you to know your child and to do what is appropriate given their level of maturity.

## School Attendance

If you are reporting for your child and they are attending school, you may optionally tell us about the school they attend, which bubble your child belongs to in addition to the other sensitive personal data collected by the app. We use this information in the same way we use other sensitive personal data, but in addition we may process this data in order to:

- Give schools insight into the health of their students, allowing faster decision making and better protection for children.
- Reassure parents that they are their school are making informed choices about their child's safety and education.
- Increase protection for children.
- Collect important information on the impact of COVID-19 on children for the purposes of wider scientific research.

## Third party processors for both kinds of information

We use third parties to process some of your personal data on our behalf. 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. They are not permitted to keep the data after our relationship with them has ended.

These processors include:

- Google Cloud Platform
- SurveyMonkey
- Segment
- Google Firebase
- Amplitude
- Google G Suite
- MailChimp
- Mailgun
- Intercom
- Sentry
- Google Firebase
- Cloudflare
- Sqreen

## Your rights

Because the work Zoe Global Limited does takes place in the UK, the European Union's "General Data Protection Regulation" (GDPR) applies to our processing of your personal data, even if you do not live in Europe. From 1 January 2021, the GDPR will be replaced, for most purposes, by an equivalent regulation specific to the UK. This should make no difference to the rights that you have, even if you do not live in the UK.

Under the GDPR you have a number of important rights free of charge. In summary, those include rights to:

- Access your personal information
- Require us to correct any mistakes in your information which we hold
- Require the erasure of personal information concerning you in certain situations
- Receive the personal information concerning you which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to a third party in certain situations
- Object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you
- Object in certain other situations to our continued processing of your personal information
- Otherwise restrict our processing of your personal information in certain circumstances

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.

## About us

Our UK address is: 164 Westminster Bridge Road, London SE1 7RW
Data Protection Officer: dpo@joinzoe.com

Institutions we share data with:

- King’s College London
- Guys & St Thomas' Hospitals
- NHS
- Swansea University (SAIL Databank)
- Harvard University
- Stanford University
- Massachusetts General Hospital
- Tufts University
- Berkeley University
- Nottingham University
- University of Trento
- Lund University
- University of Hawaii
- University of South California
- The University of Texas MD Anderson Cancer Center
- Northshore University HealthSystem
- City University of New York