

# Privacy notice

## European General Data Protection Regulation

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.

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 body temperature, height and weight)
- Information about pre-existing conditions
- Information about your symptoms
- your COVID-19 test status
- Details of any treatment you have received
- General information about you such as your sex at birth, your year at birth and your location (including postcode)
- Whether you are a health worker coming into contact with patients
- General information about you such as your sex at birth, your year at birth and your location (including postcode)

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

- Information about your diet
- What you do if and when you go out, such as where you go and whether you wear a mask or other protection

We process this data in order that:

- We can better understand symptoms of COVID-19
- We can follow the spread of COVID-19, for example so that we can identify hotspots
- We can identify the exposure of healthcare workers to COVID-19
- We can advance scientific research into the links between patient's health and their response to infection by COVID-19
- In the future we may use this data to help the NHS support sick individuals

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](mailto: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 use this information for the following purposes:

- Asking you for feedback on the app or conducting other forms of survey.
- Keeping in touch with you about the app and its performance.
- Sending you information about new versions of the app or similar apps we may have in the future.
- Identifying faults or other problems connected with the app

We will not send any emails not meant individually for you (for example marketing emails) if you do not want us to do so. Every such email will include a link you can click to opt-out from receiving them. We will not sell your contact information to third-parties.

Our legal basis for processing this information is our legitimate interest in developing, marketing and running 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.

## **Recording information for others**

The app also allows you to input information about other people in addition to your own by making a separate profile for them. If 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 your child is attending school, you may optionally tell us about their school, their bubble and other things about their attendance. We use this information in the same way we use other sensitive personal data, but in addition we may (where it would not identify any individual) use it to alert you to an infection in your child's bubble and to help the school plan for any impact of COVID-19.

## **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
- Sscreen

## Your rights

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: Zoe Global Limited, 164 Westminster Bridge Road, London SE1 7RW

Data Protection Officer: [dpo@joinzoe.com](mailto: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