



Privacy Policy

Under data protection laws, we are required to provide you with certain information about who we are, how we process your personal data and for what purposes, and your rights in relation to your personal data. This information is provided HERE and it is important that you read that information.

How you can withdraw consent

Once you provide consent, you may change your mind and withdraw consent at any time by contacting us on contact@vuidiagnostics.com but that will not affect the lawfulness of any processing carried out before you withdraw your consent.

Introduction

This policy (together with our end-user licence agreement as set out on our website (EULA) and any additional terms of use incorporated by reference into the EULA, and our terms & conditions, together our **Terms of Use**) applies to your use of:

- ViewEye mobile application software (**App**), once you have downloaded or streamed a copy of the App onto your mobile telephone or handheld device (**Device**).
- Any of the services accessible through the App (**Services**). This policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us.

1. Important information and who we are

VUI Diagnostics Limited is the controller and is responsible for your personal data (collectively referred to as "Company", "we", "us" or "our" in this policy).

We have appointed a data protection officer (**DPO**). If you have any questions about this privacy policy, please contact them using the details set out below.

2. Contact details

Our full details are:

- **Full name of legal entity:** VUI Diagnostics Limited

- **Name or title of DPO:** Simon Rabinowicz
- **Email address:** simonrabinowicz@vuidiagnostics.com

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues or other competent supervisory authority of an EU member state if the App is downloaded outside the UK.

3. Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review.

This version was last updated on 24th May 2020. It may change and if it does, these changes will be posted on this page and, where appropriate, notified when you next start the App. The new policy may be displayed on-screen and you may be required to read and accept the changes to continue your use of the App or the Services.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during our relationship with you.

4. The data we collect about you

We may collect, use, store and transfer different kinds of personal data about you as follows:

- Identity Data.
- Contact Data.
- Device Data.
- Content Data.
- Profile Data.
- Usage Data.
- Retinal Image data

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

5. How is your personal data collected?

We will collect and process the following data about you:

- **Information that you provide to us.** This Includes personal data you provide to us when you:
 - Download our app;

- Register with us;
- Create a ViewEye account with us;
- Log in to the ViewEye App and use the Services;
- Report a problem with the ViewEye App;
- Provide feedback to us.
- **Information we collect about you and your device.** Each time you use one of our Apps we will automatically collect personal data including Device, Content and Usage Data.
- **Captured Images and Associated Data.** Once your captured image and associated input information are submitted, online devices by default transfer this data to our secure third-party data server. For offline devices, such data is cached until an internet connection is established and all cached data is automatically pushed to our third-party servers.

6. How we use your personal data

The personal data that you choose to provide to us about yourself will only be used to the extent that the law allows us to do so. Most commonly we will use your personal data in the following circumstances:

- Where you have consented before the processing.
- Where we need to perform obligations under a contract we are about to enter or have entered with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Please see our Glossary to find out more about the types of lawful basis that we will rely on to process your personal data.

We will only send you direct marketing communications by email if we have your consent. You have the right to withdraw that consent at any time by contacting us.

7. Purposes for which we will use your personal data

1. **To install the App and register you as a new App user**
 - **Type of data:**
 - Identity
 - Contact
 - Device
 - **Lawful basis for processing:**
 - Your consent

2. **To manage our relationship with you including notifying you of changes to the App or any Services**
 - **Type of data:**
 - Identity
 - Contact
 - Profile
 - Marketing and Communications
 - **Lawful basis for processing:**
 - Your consent
 - Performance of a contract with you
 - Necessary for our legitimate interests (to keep records updated and to analyse how customers use our products/ Services)
 - Necessary to comply with legal obligations (to inform you of any changes to our terms and conditions)
3. **To administer and protect our business and this App including troubleshooting, data analysis and system testing**
 - **Type of data:**
 - Identity
 - Contact
 - Device
 - **Lawful basis for processing:**
 - Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security)

8. Disclosures of your personal data

You share your information as you use and communicate through our Services, and we share your information to help us operate, provide, improve, understand, support. To provide the Services we need to share your personal data with our third-party collaborators.

These organisations have been vetted by us to ensure that your information will be dealt with responsibly. These organisations are not permitted to use your personal information for any means other than to use it in accordance with our instructions.

9. International transfers

Some of our external third parties are based outside the EEA so their processing of your personal data will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see *European Commission: Adequacy of the protection of personal data in non-EU countries*.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see *European Commission: Model contracts for the transfer of personal data to third countries*.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US. For further details, see *European Commission: EU-US Privacy Shield*.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

10. Data security

At VUI Diagnostics we take security and the secure storage of personal data seriously. We encrypt and store all personal data on secure servers using the latest technologies. All information you provide to us is stored on our secure servers. Where we have given you (or where you have chosen) a password that enables you to access certain parts of Website, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Once we have received your information, we will use strict procedures and security features to try to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way.

Where personal data is stored on your Device it will be encrypted and protected by 2 factor authentication.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator when we are legally required to do so.

11. Data retention

The data that you provide to us in accordance with this policy will only be retained by us for as long as necessary to fulfil the purposes we collected it for.

In some circumstances you can ask us to delete your data: see *Your legal rights* below for further information.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

12. Touch ID/Fingerprint Recognition

Users may choose to use fingerprint recognition/touch ID as part of our Services when logging into the App. The data provided as part of this service is not stored as processed by VUI Diagnostics. Should Users have any concerns as to this, they should contact and/or review their relevant platform providers privacy policy.

13. Your legal rights

Under certain circumstances you have the following rights under data protection laws in relation to your personal data.

Your Right of Access

You have the right to ask us for copies of your personal information. There are some exemptions, which means you may not always receive all the information we have about you. You can read more about this here (<https://ico.org.uk/your-data-matters/your-right-of-access>).

Your Right to Rectification

This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us. You can read more about this here (<https://ico.org.uk/your-data-matters/your-right-to-get-your-data-corrected>).

You Right to Erasure

This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request (<https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted>).

Your Right to Restriction of Processing

This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- if you want us to establish the data's accuracy;

- where our use of the data is unlawful, but you do not want us to erase it;
- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
- you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

(<https://ico.org.uk/your-data-matters/your-right-to-limit-how-organisations-use-your-data/>).

Your Right to Object to Processing

You have the right to object to processing if we are able to process your information because the process forms part of public tasks or is in our legitimate interests. You can read more about this here (<https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/>).

Your Right to Data Portability

This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated. You can read more about this here (<https://ico.org.uk/your-data-matters/your-right-to-data-portability/>).

Your Right to Withdraw Consent

Where we are relying on consent to process your personal data. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

You can exercise any of these rights at any time by contacting us at contact@vuidiagnostics.com.

Glossary

Lawful basis

Consent means processing your personal data where you have signified your agreement by a statement or clear opt-in to processing for a specific purpose. Consent will only be valid if it is a freely given, specific, informed and unambiguous indication of what you want. You can withdraw your consent at any time by contacting us.

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our

legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

Description of categories of personal data

- **Identity Data:** first name, last name, maiden name, username or similar identifier, title, date of birth, gender.
- **Contact Data:** email address and telephone numbers.
- **Device Data:** includes the type of mobile device you use, a unique device identifier (for example, your Device's IMEI number, the MAC address of the Device's wireless network interface, or the mobile phone number used by the Device), mobile network information, your mobile operating system, the type of mobile browser you use and/or time zone setting.
- **Content Data:** includes information stored on your Device, including users' account details, login information, images or other digital content, and/or check-ins.
- **Profile Data:** includes your username and password, preferences and feedback.
- **Usage Data:** includes details of your use of any of our Apps, including, but not limited to, traffic data and other communication data
- **Retinal Image Data:** includes retinal images of both left and right eyes and medical impression annotations and disease status types