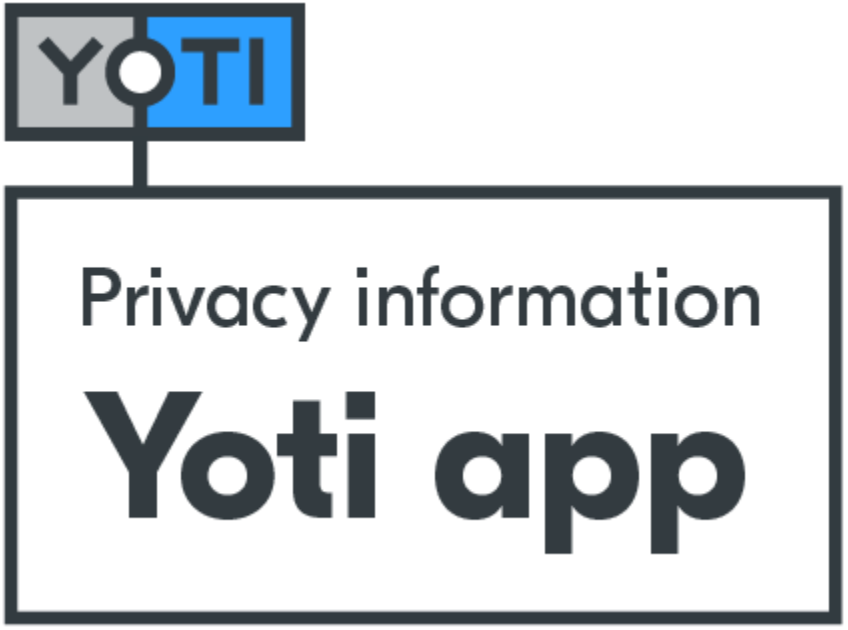
YOTI
Privacy information
Yoti app

Jump to section

Past versions

What’s new

What is it?

Yoti is a biometric identity app that provides you with a quick, easy, secure and privacy-friendly way to prove your age and / or identity, online and in person. You set it up once and then use it anywhere that accepts Yoti. It works by allowing you to share verified details (we call these attributes) from ID documents you add to your Yoti account. In some cases you can also manually add details, and have them verified.

We have some FAQs on the Yoti app here:
https://yoti.zendesk.com/hc/en-us/categories/200895765-General-FAQs

The information in this privacy notice relates to the Yoti app. We also have general information that applies across all our business here: https://www.yoti.com/privacypolicy/

That page provides information about Yoti, our business principles, our Guardian Council, contact details and general personal information collection and use practices. The page also has links to all the product-specific privacy notices.

Information collection and use

We collect information to set up your Yoti account, when you add documents and when you use the app.

We use it to do things like:

- create your account and provide the products / services;
- check you don't already have an account;
- check the document you add is genuine and the photo matches your account set-up photo;
- check you're a real live person;
- verify details;
- check for fraud;
- authenticate you when you make certain requests, such as to delete your account.

Creating an account with Yoti

Information	Use
Your mobile number	To create your account in the app.

	To check you do not already have an account with Yoti – users are only allowed to have one account. We encrypt your mobile number (which means we can't access it) and keep it until you or we close the account and delete the information.
Your photo	To have a photo on your account that you can then share. After registering you are able to take an account photo, which you can then share as part of proving your identity. We also ask you to take a photo when you take certain actions in the app, so we can be sure it's you. Organisations may also request this as an extra security step. See the section below for more information. Yoti securely stores the photos. We keep this information until you or we close the account and delete the information.

Checking you are a real person and fraud prevention

Information	Use
Your biometric template Face scan or video to prove you are a real person	The main use of your ID document information is to add the details to your Yoti account, so they are available for you to prove your ID and age when needed. When you set up your account we have a security measure to make sure you are a real person, and to make sure no-one is pretending to be you (such as by holding up a photo). This is done in two different ways and which one you get depends on things like whether your phone make and model is compatible with the different technologies, or whether there are any technical errors that prevent one technology from working. One method involves you moving the phone towards your face. The other method involves taking a short video of you saying some words. Our Security Centre check this video and it is deleted after seven days.

	The scan or video also takes a still image of you from which we create a biometric template, which we store securely. A biometric template is a digital map of your face. Whenever you take certain actions in the future and we need to check it's really you, we ask you to repeat the video or take a photo, and compare the image to the digital map. When you add a document, reset your PIN or need to recover your account (such as if you lose your phone), we take the scan of your face and video as an extra security step to verify that it is always you trying to take those actions. We automatically compare the face scan to the one you did when you set up your account. If we ask you to say some words, our Security Centre also reviews the video. We also ask you to take this extra security step the first time you use quick scan, or swap and send your details, if you have not already been through it. If you want to delete your account we ask you to take a photo. We automatically compare this to the face scan you did when you set up your account.

	The scans and video helps us to make sure you are a real live person, and prevents someone else who has access to your phone from taking the actions listed above. We delete the video after seven days. We may use some videos within the seven-day window for internal testing to improve our security checks. We use some sections of the video for internal research and development to improve our fraud prevention measures. See the section on biometrics for more information on the face scan / biometric template and research work. Sound detection: where we ask you to say some words, we collect the device model, language and sound levels during the video. We collect sound levels so we can alert you to redo the video if the sound level is not high enough. We collect device model so we can set the correct minimum sound level we require for each type of device meaning that users are more likely to get through this check more quickly and successfully.

	We collect the language set on the phone to help understand if errors and issues with this registration stage are caused by us not supporting the local language. We keep this information until you or we close the account and delete the information.

Adding information to your Yoti

Information	**Use**
Information from Government-issued or other official identity documents (for example, passport, driving licence)	We use the photo and your date of birth (which we hash) to check if your identity already exists. Users can only have one account. (Hashing means turning the actual information into a string of numbers and letters to hide the real data. For example: 85da15a402360fe8ad2e80d958ded300ac9ffb955e3d7cff89007bb340e2b8d5) We use the information to verify your identity and check the document is valid. You will not be able to add an expired passport or driving licence.

	If your document has a date of birth we check this to make sure that it matches what you told us when you were asked about your age as part of setting up your account. If you are below a certain age in some countries you need parental consent to use the app. We don't currently have a parental consent mechanism in place. We check the document photo against the photo you took to set up the account, to check it's your document. It may be sent to our Security Centre for a manual check. If your passport has a chip in it, and your phone has NFC, our technology is able to read the information on your passport chip directly. NFC stands for Near Field Communication. It allows your phone to interact wirelessly with something else that is very close by. It is the same technology behind contactless cards and paying for items using your phone. Using this method allows us to check your passport has not been tampered with and provides a better quality photo for our security checks.

	CitizenCard If you upload a CitizenCard, we will verify your name, date of birth and CitizenCard number against the CitizenCard database. When they confirm your details to us they also send us the photo and gender they have for you. We check the photo against the face scan we took when you set up your account to make sure it's really you. We add your gender as an attribute. **US driving licence and state ID** For these documents we check against the AAMVA database (American Association of Motor Vehicle Administrators). We verify name, document number, issuing authority (State), gender, address, date of birth, expiry date and issue date. AAMVA sends back yes / no for each field. We then consolidate this into one or two overall yes/no answers (one general match decision, and one address match decision). Not all US States provide data to AAMVA and some that do restrict who can receive it, so we may not get a result for you. AAMVA information on participating States is here: https://www.aamva.org/DLDV/ (participants tab).

	Fraud checks We check your document information against information from the Metropolitan Police Service Amberhill Identity Team in relation to false identity documents / information. We may also check your document information against the Cifas fraud prevention database. The results of these checks could lead to you not being able to upload your document. In cases of serious document or identity fraud we may have to prevent you from setting up a Yoti. We keep fraud information either in line with our internal fraud and misuse policy or the retention rules set by relevant fraud prevention bodies. If we file a fraud report with Cifas, they will keep your information for up to six years. See the section on information sharing for more information. **Specific Yoti uses** While we verify your identity we keep the information securely but our Security Centre can access it, and may do so for training, compliance and quality assurance purposes. We can only access this information up to seven days after verification. If we suspect fraud or other unlawful activity we may need to move your information to a separate

	secure area and we will keep this information for as long as we need it to investigate. Where we identify fraudulent or tampered with documents, we will keep some for up to two years as examples to use in internal staff training and to train our software to better detect false documents. Where you upload a passport using its chip (as described above), but the upload fails, our technical support team are able to access the information for up to seven days to analyse why it failed and to create a fix to prevent future failures. The data is encrypted and can only be accessed on a secure server through a VPN. Very often, an upload fails because the country that issued the passport has configured the chip details slightly differently. **After you successfully add a document** We then add the details to your Yoti account and keep this information encrypted on our servers (which means we can't access it) until you or we close the account and delete the data. Your details include an image of your document, which you can share where a company requires it, such as for KYC or anti-money laundering checks.

	Adding multiple documents You can only have one document of each type at any one time. So if you add a passport and then want to add a second passport, the details from the second one will be listed in your account and available to share. The details from the first one will still be there but you will not be able to share them. **Statistics** We create general statistics and reports from some of this information to help us understand how people are using our app, and to allow us to improve the service. This information does not identify any specific user. See the sections on analytics for more information.
Information you add manually (for example, address, e-mail)	If you add an email address we will verify it by sending you a code. If you add an address you can choose to verify it with a third party. If you don't verify it, or the check fails, your address will be marked as 'unverified'. You can still share it, but some organisations may only be able to accept verified addresses. In these cases we will ask you to verify your address so you can share it.

	Third-party checks: In the UK this is TransUnion. This will leave a footprint on your credit file, which does not affect your credit score. For other countries this is ‘Aristotle Integrity’ service. We keep the information until you or we close the account and delete the information.
Yoti age estimation	You can use our age estimation technology, Yoti Age Scan, to estimate your age. That way, you can prove your age without adding an ID document to your Yoti. Yoti Age Scan instantly estimates whether you're above a certain age threshold, such as 18+. It doesn't estimate your actual age. It works by using the digital map of your face we captured when you created your Yoti. When you choose to use this feature in the app we send a copy of the digital map of your face from your Yoti to our servers. After the age estimation we permanently delete it. Your original digital map is stored securely. We add your estimated age to your Yoti so you can use it to prove your age. Some businesses will accept an estimated age as proof of age to access age-restricted goods and services.

	You can remove your estimated age from your Yoti at any time by replacing it with your date of birth from an ID document. When you look older than a certain age threshold, Yoti Age Scan can confidently estimate that you're above that age once it takes estimation errors into account. If you get an error message it might be that you look too young for Yoti Age Scan to confidently estimate that you're over 18, which is our minimum estimated age threshold. You can read more about our age estimation technology here: yoti.com/age_scan_wp
Aadhaar	**Scanning your Aadhaar card** You can add Aadhaar information by scanning the QR code on your Aadhaar card. This includes your full Aadhaar number but only so we can check the format is valid. We then obscure all but the last four digits. You can manually add your full date of birth if your Aadhaar card only contains your year of birth.

	We do not carry out any checks on your information and while organisations receiving details from you will know they came from your Aadhaar card, the details will not be verified. **Uploading your Aadhaar file** Once you have downloaded your Aadhaar file from the UIDAI website you can upload it to Yoti. You have to upload the whole file as UIDAI don't provide the option to select details to share. We only convert your name, address, date of birth and gender to attributes you can share. We will also need your share code to open the file and upload your details. When we ask you for access to your files this is only so we can alert you when the download is complete and to upload your details. For security we check: ● the photo on your Aadhaar file against the one in your Yoti; ● your mobile number against the one on your Aadhaar file; and ● your mobile number and the last four digits of your Aadhaar number, to make sure you haven't already uploaded this.

	We don’t see your email or full Aadhaar number. The file only contains the last four digits of your Aadhaar number. The only information we store are the attributes and phone number. The phone number in your Aadhaar file is hashed, which is a security measure to protect the actual data so it appears as a string of numbers and letters. When you provide your full number as part of uploading the file we can carry out the same hash technique and check the results match. We do not keep the hashed version. We keep the full number you provide as so we can make sure you can only upload your details to one Yoti account. If you replace verified Aadhaar details with unverified ones, you will archive the verified details and could lose some of them.
Updating your information	When you add an updated ID document (such as when you renew your passport) the details from the new document will be in your account. We will archive the old document details. If you update your address by manually adding a new address, we will archive the old one.

	If you update your address by adding a document that includes it, all the other details from that document will also appear in your account. We will archive the details you previously had, except for ones that do not also appear in the new document you add. If you update your mobile number, the new number will replace the old one. You will be sent a code to verify the new number.
Age attribute (for example, 23 or 18+)	We are able to convert your date of birth into an age attribute so that in some circumstances you won't need to share your date of birth to prove your age or eligibility for a product or service.
Yoti ID	When you add an ID document we turn the name and photo into a digital ID card that you can show on your phone. To quickly and easily share your verified name and photo with another person or organisation, you can choose to let another Yoti app user scan the QR code on your card. This has the added benefit of confirming to the recipient that your ID card is a genuine Yoti ID.

Adding information from third parties

You can store information from third parties in your Yoti account. For example, information from your employer, from an organisation you volunteer with, loyalty card information, or medical certificates.

This can allow you to have trusted and verified digital credentials in your account, and allows you to use your phone as a digital ID card.

Yoti partners with trusted organisations for this, and they will provide you with information on how they want to use Yoti for digital ID or credentials.

In some cases the organisation will need to provide Yoti with a list of authorised individuals who can get the ID or credential information on their phone. In some cases the organisation may provide Yoti with an API to check data on their own systems. In some cases the technical setup may allow the data or credential to be automatically sent to your Yoti following an action.

The app will provide instructions and contain relevant information for the different scenarios. Here are some examples.

- An organisation uses Yoti to provide a digital ID card the person can show on their phone

When you go through the registration process and enter details such as your e-mail address, mobile phone number, or other information as needed (such as an employee number or other identifier), we will check this against the list provided by the organisation. If the details match, we can issue the information or credentials to your Yoti account.

You will then have these available as an ID card you can show. When you show your ID card, it also contains a QR code that an organisation can scan to check the ID is valid and receive the ID details.

The organisation can update and delete the list at any time, such as if details change or they need to revoke a credential.

- An organisation offers Yoti as a way to receive a medical test result

If you choose to use Yoti for this purpose the organisation will present you with a QR code so you can share some identity details for the test, and they can link your details to the specific test you take. Your result is sent straight to your Yoti app and you will get a notification when it is ready.

The result will be securely stored on your Yoti where only you can access it. When you need to prove your test result, you can display it in person or share it remotely with a business that requests it.

Yoti cannot access this third-party information and does not do anything else with the information provided. We store it securely.

You can view this information in the app at any time and it is included if you use the ‘download my data’ function.

Resolving document issues

You can only have one Yoti account and so you can only add your ID document to one account. If you try to add a document that you have already added to another account you will see a message about

releasing your document. This means deleting the current record of the document in our system and blocking your old account. Once done, you will be able to add the document to the Yoti account that you were trying to add it to.

For security, we will need to verify that you own the document and the old account, so we ask you to take a photo and compare it to the digital map of your face set up when you created your account. (See the section on ‘Checking you are a real person and fraud prevention’ for more information on the digital map.)

In the app when you tap to release your document, we will start the process of blocking your old account. We cannot reverse this. If you still have access to your old account you may want to save any data from it, as you won’t be able to access it once it’s blocked. To learn more about saving data, see our FAQ here: https://yoti.zendesk.com/hc/en-us/categories/200895765-General-FAQs.

Once blocked, other people will no longer be able to swap or share details with your blocked account.

As we have architected our system to have no access to user data, when we release your document and block your old account we can’t delete the data from your old account. When you add a document we create a one-way hash of it, which is a security technique to protect the actual data so it appears as a string of numbers and letters. When you try to add the same document again we can carry out the same hash technique and see if that document already exists in our system. If it does, to release it, we delete the hash, so that when you try to add it again, our system doesn’t flag that it already exists. This

means the data from your old account cannot be accessed or used by anyone in any way. Data in our system that has had no activity on it for three years is deleted.

Recovering your account

If you want to be able to recover access to your account, such as if you lose your phone or reinstall the app, you will need to set this up by allowing us to store an access key in iCloud or Google Drive. The app will ask you for permission to access your iCloud or Google Drive, but this is only so we can store the key there that we will need for you to recover access to your account. We do not access anything else stored there and you can turn off the sharing permission once the set up is complete. When you want to recover your account, if we don't have the access permission, we will ask for it again so we can retrieve the key to restore your access.

Information	**Use**
The access key from iCloud or Google Drive	We retrieve this to restore access to your account.
Face scan and video	To verify your identity and check you are the true holder of the Yoti account and grant you access to it again or to allow you to reset your

	PIN. See the section on ‘Checking you are a real person and fraud prevention’ for more information. If you forget your PIN we will ask you for your mobile number and date of birth (if you have added a document). While we verify your identity we keep the information securely but if we need our Security Centre to review the video, they and the Customer Support Team can access it. We can only access this information for up to seven days after verification.

Deleting your account

You can delete your account from the app settings. It is important to note that if you delete the app before deleting your account, you don’t delete your data, you just lose the connection to your data, and it remains ‘orphaned’ in our system. This means the data cannot be accessed or used by anyone in any way. We delete orphaned data after three years.

Using your Yoti

Information	Use
App login details	To log you in to your Yoti
Information about issues and problems you have with the app	If the app crashes, or you have some other issue, you can contact us about it by email, from within the app or through the website. If you click on a 'contact us' or 'help' button in the app, the email you send is prefilled with some diagnostic information: platform (iOS / Android); device model (such as, Samsung Galaxy S7); device OS version (such as, iOS 10); the Yoti app version and what country you are in (based on your mobile country code). You can delete this before you submit your email. This information helps us identify what went wrong. The information you send comes to us by email and, if you have an email address on your Yoti account, you will receive an acknowledgement email with a ticket number for your issue. This creates a Yoti Customer service account for you so you can revisit your ticket(s) to see progress and contact us further about the issue or any other issue.

	Once we have resolved your issue and / or closed the ticket, we will send you an email asking for feedback. We only use this information to improve our services. We delete the support tickets after six months. When you have a problem with the app we use a Request ID to help us find the server logs for your phone so that we can identify and fix the issue. The server log is an automatically generated list of things that happen when you take actions. For example it records that a call was made to a particular server and how long the server took to respond. It also records successful and unsuccessful actions like login, adding a document and so on, and the reasons why an action failed. Understanding what happened in what order and where failures happened helps us determine what went wrong and how to fix it. On the back end, the app associates your server log information with a Request ID (for example, 3bbf6e6fe414b40bf9fed99c8d36bd2c). When you contact us through the app, the message automatically includes the Request ID and the last 20-40 actions. When you email

	us from help screens we ask you if you want to include the server log information. We also use Crashlytics which sends us information automatically when the app crashes or has other issues. Crashlytics create a unique user ID that they attach to the crash reports. The report tells us the device make and model, operating system, the disk space and memory space left, whether the screen was portrait or landscape and whether the device is rooted. This information helps us understand what issues there are and whether they are device specific or as a result of the device setup. We do not see or have access to the unique ID. We have no way to identify any specific user. Crashlytics delete all the data after 90 days.
Anonymous information that does not identify any specific user about what types of information you have shared with third parties	This information allows us to charge organisations for the information they get from you. For example, we may charge an organisation more for receiving five pieces of information from you through Yoti, than we would charge an organisation who only received three.

Certain device or user information (such as location, photo)	Some uses of Yoti require us to carry out authentication or fraud prevention checks to make sure that it is really you.
Rate Yoti	When you complete certain actions in the app we may prompt you to rate the Yoti app. Any rating you give is anonymous. We may also prompt you to rate us in the app store. For negative ratings we will ask you if you want to send us comments or feedback. If you choose to do so, this will open a feedback form so you can send us an email.

Push notifications

After you add a document to your Yoti you can choose to allow push notifications. We have three types of push notifications which you can turn on or off in our app settings.

Account updates: to notify you when your video, document or details have been reviewed. These notifications are automatically generated when the action is complete.

Details shared: to notify you when you successfully share your details. These notifications are

automatically generated when the action is complete.

Reminders: to notify you when you have an action to finish. The notifications you get will depend on what actions you have started and completed. Please also see the ‘Analytics’ section for more information.

Information sharing

You choose if you want to use Yoti to share your information with other individuals or with companies. You will get a receipt of any sharing you do.

- Where we have access to your information, we may share it in specific circumstances, such as:
- suspected or confirmed identity fraud or other offences;
- valid and legally binding requests for information from third parties;
- to verify your details;
- where a company you are sharing details with requests further checks with third parties that we are able to provide.

We do not sell your information.

When Yoti shares your personal information

While we verify your account, for a short period of time after you register or add information, your account will be pending and Yoti will be able to access your personal information. Usually this is only for seven days, but we may need to continue to store it and access it where we suspect or find fraud or other unlawful activity.

Yoti's core principles are that it is not our business model to sell, transfer or share outside the company any of the personal information used to set up your account or your user activity information.

There are some situations where we will share or will have to share some information, and we list these below.

Situation	**Who we share your data with**
If we suspect a registration may involve identity fraud, a national security threat, legal infringement, or a criminal offence	We may have to share a copy of your information with the appropriate authorities.
If you provide false or inaccurate information or present a false document	We may pass a copy of your information or an image of the false document to the relevant fraud prevention agencies, law enforcement agencies

	or the organisation who issues the genuine version of the false document. If, after investigation, we determine that there has been fraud that meets the criteria for reporting to Cifas, we will pass on the details to prevent further fraud and money laundering. Cifas keeps fraud reports for six years. Other Cifas members may use the information we report to refuse to provide you with services, financing or employment. You can find the Cifas privacy information here: https://www.cifas.org.uk/fpn. We also work with the Metropolitan Police Service Amberhill Identity Team in relation to false identity documents / information.
If we get a request for user information from a law enforcement or other official authority	We cannot provide your information that is encrypted in our database unless either you, or a third party you shared your information with, provides us the receipt from your sharing activity,

	as this contains the decryption key necessary to access the personal information you shared with that third party. We have an internal policy and process to make sure that, where we are able to share information, the request is valid, the information requested is no more than necessary, and that we think it's the right thing to do. We may have a legal obligation to share the information if we receive a court or similar legal order ordering us to disclose it.
If you have provided your address	We will check this information against a third party as part of verifying your identity. Please see the section on 'Adding information to your Yoti' for details of the third-party checks we carry out.

Some companies using Yoti will request an identity check against credit reference agency or other fraud prevention data	In these circumstances Yoti simply sends the relevant details to the credit reference agency or fraud prevention database on behalf of the company, and sends the response back to the company.

When you share your personal information

You alone will decide when you want to use your Yoti to identify yourself to a third party, or to swap, send and request information. You choose whether to agree or not to share the information the third party requests. If you decide to share your information with a third party, you will both receive a receipt which will contain a copy of the information that each party shared.

Yoti encourages companies to only ask for the information they actually need, for example, your age, or confirming you are over 18, rather than a full date of birth. If you choose to share your information with a third party using Yoti, those third parties may choose to use that information to communicate with you or they may share that information with others. We suggest you read the privacy policies of any organisation you share your information with to understand how they will use your personal information.

Yoti creates and encrypts a master receipt which contains the details of what information was shared and who with. This master receipt is securely stored on our servers and we cannot access it unless either you or the third party provides us with their own receipt containing the encryption key we need to access the information.

You can access your sharing receipts in the app, and also by logging into Hub: https://hub.yoti.com Please see the Hub product section for relevant privacy information.

Organisations using Yoti can request the source of the information they request from you, such as ‘passport’, ‘driving licence’ or ‘unverified’. This is because some organisations carrying out some types of identity checks are required to evidence where they got the details from.

Remember Me IDs

When you allow a share with an organisation, Yoti generates two unique Remember Me IDs. One is for the specific service you are using, and one is for the organisation that owns that service. It means you don’t have to share your personal details every time, as the organisation or service can just ask for your Remember Me ID instead. The service and any other services owned by the same organisation will already have your personal details if you have shared them using Yoti in the past.

For example, if you use Yoti to prove your identity with service 1 offered by Company ABC, that share will contain one ID for service 1 and a different ID for Company ABC. If you then use Yoti to prove your

identity with service 2 offered by Company ABC, that share will contain the same Company ABC ID and a different ID for service 2. Yoti has no access to these IDs.

The service or organisation can choose to store these IDs along with the personal information they request from you. If they store it, they can use this ID to recognise your Yoti when you share with them again, so you can use different services or features without having to keep sharing the same information for each interaction.

For example, if you register with a site using Yoti the website can use the ID to allow you to log in to the site, prove your age, carry out 'know your customer' due diligence and so on, by only asking for any required additional details, rather than asking you for all your details again. This approach is in line with Yoti's data minimisation principle, meaning you should only share the details relevant to what you are doing.

If an organisation or service you are sharing information with uses the ID and you do not want them to do this, you should contact them to delete your account with them. The IDs are unique to your Yoti account, so if you delete your Yoti account you will lose your IDs. If you then set up a new Yoti account you will have new IDs which will not be recognised by any organisation or service you previously used with your old Yoti account.

If you allow a share with another individual there will only be one Remember Me ID.

Always allow

We provide a feature to some companies, for some scenarios, where you can choose to automatically share the same information each time you interact with them. Usually, you scan a QR code to see what information the company is asking for, and you are asked whether you want to allow the sharing of your information. With ‘Always allow’ you can cut out the approval step. This may be useful to save time for some transactions you carry out often, where the same information is requested from you each time.

Security and data location

The information you provide is stored separately and encrypted in secure locations. Once your account is set up, we have no access to your information. Only you have access to use the app to share your information as you choose.

We continually test our systems and are ISO 27001 and SOC 2 compliant, which means we follow top industry standards for information security.

Your encrypted information

Except for the biometric template and photos, as mentioned in the ‘Information collection and use’ section, we do not have access to your personal information that we have verified and stored on our servers. The only way we can access the information is if you provide us with the encryption key (which is a set of unique numbers stored securely on your device). Only you hold the keys to decrypt your account information.

Sending your personal information to other countries

We keep all the personal information you add to your Yoti in the UK in a highly secure datacentre. All the information is held separately and encrypted.

We have a Security Centre in India who carry out the same fraud prevention checks when you set up your Yoti as our UK Security Centre. The personal information does not leave the UK, the India Security Centre have secure remote access to carry out their role. We have EU-approved model contract clauses in place between Yoti UK and Yoti India.

If we decide or are obliged to send or store your personal information in another country, we will update this section to describe the protections we have put in place.

Biometrics

Biometrics are your unique features, such as your face. We use biometrics in our app to help prevent fraud and to make sure it's actually you using Yoti. Yoti is a biometric identity app, so you can't use the app without this extra security.

We also use some user data in our internal research and development (R&D). For some projects this could include your biometrics. You can opt out of this in the app settings.

When you set up a Yoti account we ask you to consent to our use of your biometrics. You can withdraw this consent at any time in the app settings. You can opt out of R&D data use, which will allow you to continue to use the app.

What are biometrics?

Biometrics is the measurement and analysis of your unique physical characteristics and behaviour, such as your face, your fingerprint, your voice, the way you walk, the way you use your phone and so on.

Legally, biometrics is defined differently in different laws, but the common factor is that you are identified or authenticated through your unique physical characteristics or behaviour. Not all Yoti uses

of this data identify or authenticate you. However, to make things easier to understand, we have called all the physical characteristics and behaviour data ‘biometrics’.

Some data might involve your face, for example, or elements of your face, but without identifying you. For example, we have developed technology to check if a face presented to the app is real, or if it is someone wearing a mask. This activity doesn’t identify you in any way, it checks the image is genuine.

Where we do need to identify or authenticate you, using biometrics allows you to prove it’s really you by comparing your characteristics with a template you have already set up or that has been created for you automatically. The template is created and stored securely and then each time you need to prove that you are really you, your information is compared against the template to see if it matches.

For example, many smartphones allow access using a fingerprint or your face, instead of a PIN. To use your fingerprint or face you first need to provide it to your phone so it can create a template. Then every time you use your fingerprint or face to access the phone it compares it to the template and only lets you in when the fingerprints or face match. This prevents someone else from accessing your phone.

Apps like Yoti can use the phone’s fingerprint or face technology so you can log in to our app using your fingerprint or face instead of your PIN. We don’t collect or store your fingerprint or face to do this.

Why do biometrics provide more security?

Instead of having to remember PIN numbers, or usernames and passwords (which may be guessed or hacked), biometrics uses something unique to you that only you have, like your face or fingerprint. Many companies, such as banks, are using biometrics like voice recognition to make sure only you can access your account.

Why does Yoti use biometrics?

Yoti is a biometric identity app. It works by allowing you to set up a trusted, genuine and verified digital identity. The biometrics are a key part of making sure we keep out fake identities and documents. The biometrics also make sure that it really is you taking actions in the app.

Essentially, our use of biometrics to identify or authenticate you is to prevent fraudulent use of Yoti and protect your data.

We also use some user data for internal R&D, which is explained under the ‘Internal research and development’ heading.

What biometrics does Yoti use and why?

Face

When you set up your account we take a scan of your face to create a biometric template of your face, which we store securely. A biometric template is a digital map of your face.

When you take certain actions in the app and we need to check it's really you we will ask you to take a photo or take another video and compare it against the template to check it matches. We also check the image is of a real person. These checks make sure that only you can take these actions. We usually ask for these checks when you want to take an action that would have a negative impact on you if it wasn't really you. For example, changing your PIN or deleting your account.

You can also add an ID document to Yoti so that you can share verified identity details like your name, address and date of birth. When you add a document we compare its photo with the face template to make sure users only upload their own documents, and we check the image is of a real person.

Checking you're a real person

When you set up your account, add an ID document or take other actions in the app that need extra security, we need to make sure that it's really you and not someone pretending to be you. We use different technologies for these checks. Some ask you to take an action, such as moving the phone towards your face or recording a short video of yourself saying a few words. Some happen in the background automatically. We use the information from these checks to make sure you are a real

person. We can’t give you any more details about how this works, as we don’t want people to be able to get round our checks.

Internal research and development

As well as preventing fraud in your everyday use of the app, we need to make sure our security checks continue to work and that we constantly improve them so we stay ahead of fraudsters and others who might try to provide fake identities or might try to get into your account.

We have an internal research and development team who are constantly testing new ways to prevent fraud, and to do their job they need real data from real people.

When you set up your Yoti account and add an ID document we collect certain data for R&D purposes. We can’t provide too much detail of exactly what we collect and exactly how R&D use different data, as we don’t want people to be able to get round our security and fraud checks. However, all R&D have are things like the country code of your mobile number (example: +44 = UK), photos, or sections of the video or phone movement measurements. The country information helps us for things like selecting relevant and representative data and understanding anomalies, issues and inconsistencies in results.

To test and improve our age-estimation technology R&D need images of faces and the verified age of that face. So they use photos you take for your Yoti account and still images from the video. For the verified age they use year of birth from an ID document you add that contains this information). They also get gender if that is on the ID document. This is used to prevent bias as set out below.

Our age-estimation technology is an app feature so you can have an estimated age to share with others, before you add or instead of adding an ID document (that has a verified date of birth on it). We also offer our age-estimation technology to some organisations who need to check ages. For example, when buying age-restricted products or to view age-appropriate content online. We have published and regularly update a white paper on our age-estimation technology, available on our website.

Tackling accuracy, bias and duplicate data

R&D follow accepted research good practice and manually tag some image data with information on gender, skin tone or other features. Having these tags makes sure our research data is balanced and representative. This is an important part of making sure our research results are free from bias and our technology works for everyone. It also means we can accurately report on how well it works for different groups of people.

One of the other challenges for R&D is duplicate information, for example when users delete their accounts and set up another one. To detect and eliminate duplicate data R&D receive a hashed version of your mobile number. The hashing means the number is represented as a string of letters and numbers so R&D never see your actual number and have no way to find it out. This allows R&D to determine if this string of letters and numbers already exists in their database so they can detect and eliminate duplicate data.

Can your R&D team identify me?

The R&D team don't have any other information about you, and none that could identify you personally. They can't use the limited information they have to uncover your identity or find any specific user data, which is stored separately and encrypted in our main database. We keep information used for R&D purposes on a separate R&D server, with strict access controls, for as long as it is relevant to the specific project.

What if I change my mind and don't want you to use my biometrics any more?

We hope you understand why biometrics are an essential security part of our app, but if you change your mind you can withdraw your agreement at any time by deleting your account in the app settings. There isn't a non-biometric version of Yoti, so without biometrics the app just doesn't work.

You can opt out of having your data used for R&D purposes in the app settings. This will allow you to continue to use the app which will include the essential biometric security features. Opting out means that your data will no longer be sent to R&D and any data we already have that is available for R&D to use will be deleted. Please note that if your data has already been used to train or develop a model or machine learning algorithm, it is not possible to extract your data from that model.

Your rights and choices

- You can see all the information we hold on you in the app
- If you need to update information you can do so.
- You can opt out of certain analytics in the app.
- If you want to delete your information, you must use the ‘delete account’ option in the app. If you just delete the app then the link to your information is lost and it will remain in our system with no way to find it.

Please see below for the rights that apply to Yoti app personal information.
For the purposes of the California Consumer Protection Act, we do not sell your data.

Please send any rights requests to: privacy@yoti.com

Access rights

You are entitled to know what personal information we hold about you and to receive a copy of it.

We do not have access to your personal information that we have verified and stored on our servers. The only way we can access the information is if you provide us with the encryption key (which is a set

of unique numbers stored securely on your device). Only you hold the keys to decrypt your account information.

You can access all the personal information in your account through your Yoti app. You can get a copy of this information by using the export data function in the app settings. You can also see your sharing receipts by logging into Hub. You can get a copy by taking a screenshot or by using your browser's 'Save as' function, and organisations can download their copies of share receipts.

If you have contacted our Customer Support or had other contact with us leading to us holding information on you, you can make an access request to: privacy@yoti.com

When you use your Yoti, we collect some information about your phone and how you are using the app. This information is collected and stored automatically through in-house and third-party tools, as set out in the 'Analytics' section.

Adjust analytics
We get Advertising IDs from Adjust along with event information such as 'installed app', 'completed registration' and so on. If you want to access this information about your device, you will need to provide us with the Advertising ID from your phone, as that is the only way we can search for the information.

In-house and Firebase analytics

The information we collect is de-identified and combined together (aggregated) and it is not possible to search or get the information using your name or your phone's identifiers (for example, the IMEI number which is like a serial number for your phone). So we cannot provide you with this information as it is not linked to you specifically.

Correction rights

You are entitled to correct personal information we hold about you that is inaccurate.

If you think that any of the information in your Yoti account is not accurate, you can take steps to correct it. You can manually add an address, archive old addresses and change your email. You can also simply replace an outdated ID document. You can also delete your account and set up a new one. Yoti only has access to the information in your account for up to seven days after it is first provided to Yoti.

If you change your name, you can currently only update your Yoti by adding a document with the new name.

If you have contacted our Customer Support or had other contact with us and want to make a correction request, please email: privacy@yoti.com

Deletion rights

In certain circumstances you are entitled to ask us to delete the personal information we hold about you.

Please see the ‘Updating your information’ section under the ‘Information collection and use: Adding information to your Yoti’ heading for more information on archiving documents or replacing your details with new ones.
If you want to close your account and delete your information, you can do so from within the app. You may also find these FAQs helpful:
https://yoti.zendesk.com/hc/en-us/sections/202203845-Managing-my-Yoti-account

If you have any other deletion request, please email: privacy@yoti.com

Objection rights

In certain circumstances you are entitled to object to Yoti processing your personal information.

Based on how this right works, and the choices you have in the app settings (such as to withdraw consent to biometrics, delete data or the app, or to turn off analytics), there are unlikely to be any other circumstances when this right applies. If you want to contact us about your objection rights, please email: privacy@yoti.com

Restriction rights

In certain circumstances you are entitled to ask us to restrict our processing of your personal information.

You can ask us to do this if:

- you dispute the accuracy of your personal information;
- our processing of your personal information is unlawful but you prefer restriction to deletion;
- we no longer need the information but you need it for legal reasons; or
- you have objected to our processing and we are still dealing with this objection.

If you want to contact us about your restriction rights, please email: privacy@yoti.com

Portability rights

In certain circumstances you are entitled to receive the personal information you have provided us in a structured, commonly used and machine-readable format.

This right is most likely to apply to information you have provided:

- to set up and use your Yoti;
- so we can respond to you; or

- so we can deliver the app features you want to use.

You can download the personal information you have added to your Yoti account from the app settings.
If you have contacted our Customer Support or had other contact with us and want to make a portability request, please email: privacy@yoti.com

Complain to the ICO

You can also complain to your local privacy regulator.

As a UK company, we are regulated by the Information Commissioner's Office (ICO) who is responsible for making sure that organisations comply with the law on handling personal information.
https://ico.org.uk/global/contact-us/

Analytics

Understanding how people use our app is essential. We need to know what's working, and what isn't, so we can improve. As a business, we need to know how many people are using our app, where they are in the world, and which features are most popular.

We collect information about your device and your use of the Yoti app using in-house and third-party analytics. We de-identify the information we collect so we can't identify you personally. We also combine information so that no analytics report is ever about an individual user. Unlike most other companies, we don't build individual profiles of the people who use our app. We simply look for trends and patterns to inform business decisions.

You can opt out of certain analytics in the app. Some information is generated automatically when you use our products, and we can't turn this off.

See the 'Analytics' heading in the 'General' section for information on what analytics are, why we use them, and your choices.

See below for the specific analytics we use in the Yoti app.

Adjust

We use Adjust performance and analysis technology in our app. This allows us to us to track and analyse which marketing channels or sources, and which adverts, are producing the best results in directing users to download the Yoti app, and to help us understand how our users are using our app. Adjust collects information on which ad you clicked on and on which site, and whether you installed the app. If you install the app, Adjust also collects information on when certain events happen (such as completing registration, successfully adding an ID document, first use of Yoti Password Manager).

To provide this service, Adjust uses two identifiers which they anonymise using a technology called ‘hashing’. Hashing means turning the actual information into a string of numbers and letters to hide the real data. For example: 85da15a402360fe8ad2e80d958ded300ac9ffb955e3d7cff89007bb340e2b8d5).

One identifier is the Advertising ID that Apple or Android gives your phone (depending on which operating system your phone uses). The second identifier is your IP address which is like an address for your phone from your mobile network provider, and which may change if you take your phone to a different location. Adjust hashes these identifiers. Adjust then provide us with a list of Advertising IDs and country location (based on IP address). We filter the Advertising IDs by things like country, iOS or Android users, or events such as ‘completed registration’. We then pass relevant Advertising IDs to advertising partners to be able to show our adverts to the right people on their platforms. Once the advertising partner receives the IDs they hash them. The only information Yoti has is the Advertising ID from your device and the events associated with that ID.

We use Adjust with different advertising networks that allow us to show Yoti adverts on these networks. Adjust also pass back the Advertising ID to these networks so they can build 'lookalike marketing models'. This activity is how companies make sure they target their adverts at the right types of users, and users see adverts that are most relevant to their interests. The advertising networks use the Advertising ID and any associated information they have to create groups of people who share similar characteristics. They use these groups to deliver targeted ads. They use the information they have about you to determine which groups you are in, and so which adverts you see.

Yoti uses advertising networks to make sure we only show our adverts to the people who are most likely to be interested in our products and services. The advertising networks also use the Advertising IDs as a suppression list, to make sure they don't show Yoti adverts to people who have already installed the app. See the relevant section of Adjust's privacy notice for more information: https://www.adjust.com/privacy_policy/

Opt out of Adjust analytics for all apps using their technology: https://www.adjust.com/opt-out/

You can opt out of Yoti using Adjust analytics in the app settings.

In-house and Firebase analytics

Using our in-house software, including Firebase Performance Monitoring, we collect some information from users and some information on when certain things happen as you use the app. This information

includes information about your phone, such as make and model, operating system, app version and screen size information. Our in-house software does not identify you personally.

We have two types of in-house analytics when you are using our products: information created when you take actions on your device; and information created automatically by our internal systems when things happen.

Examples of information created when you take actions on your device.

- Clicking buttons or links
- Adding documents (our analytics don’t collect any personal details from the document)
- Errors
- Completing steps, such as registration

Examples of information created automatically by our internal systems when things happen.

- App login completed / failed
- Account deletion completed
- Driving licence rejected / Passport accepted
- Sharing request started / completed / failed

You can opt out (in the app settings) of Firebase and our own in-house analytics to collect information created when you take actions on your device.
We cannot turn off the information that is created automatically, so you cannot opt out of this.

Our in-house analytics assigns a randomly generated identifier to each user, with a different identifier for each product used. (The Yoti app includes Yoti Password Manager. The identifier for this will be different from the identifier for Yoti Sign, for example.) This means we cannot cross-reference the identifiers to understand what different Yoti products you are using. We use an identifier so we can understand things like whether a count of certain actions is one user repeating an action, or multiple users each doing the same action. This helps us to understand things like where many users are having problems.

Even with the identifier, we take steps to make sure that the information we collect is de-identified so that it is not associated with an identifiable user. We do this by automatically deleting information, such as information that relates to an individual, device IDs or detailed location information. We don't collect more information than we need. For example, we collect a country location from the device, so we do not need to collect your IP address or other detailed location data to get this information.

The information from our in-house analytics and Firebase provides us with statistics on things like:

- the number of people installing the app;
- the number of accounts created successfully;
- how long it takes on average to carry out certain actions in the app, such as taking a photo, uploading a document;
- how many addresses are uploaded from a document and how many are manually added;
- the number of recovery files set up, account recoveries, and account deletions;

- the percentage of people who stop using the app at certain key points, such as accepting the terms and conditions, taking a photo and so on;
- the number of users per country, age band, and gender.

These statistics are crucial for us to understand how our app is performing, where things are failing, and what kinds of users we have. This information helps us to understand where we need to focus our business, marketing and product development efforts and what app improvements we need to make.

You can find more information about Firebase here:
https://support.google.com/firebase/answer/6318039

AB testing

We also use in-house analytics information to carry out AB testing. This is where some users may see slightly different information or screen layout. We do this to test planned improvements and see whether what we have planned makes a positive difference to the user experience. Sometimes we randomly show the different content to different users. Sometimes we use the analytics information about what actions users take in the app to only show alternative content to some users, such as those who have added a document.

If you have turned off analytics in the app settings, you may still see alternative content, but we will not be able to track how you interact with the content. We aggregate the tracking information to see which content is more successful.

Push notifications: reminders

We use analytics information to determine when to send reminder push notifications, what reminder to send, and which users we send it to. For example, if you have started to upload a document and not completed the action, we may send you a reminder to complete the document upload. If you turn off analytics in the app settings, then we will no longer receive updated information about your actions in the app. We won't send reminders to users with analytics turned off to make sure they don't get reminders that are not relevant to what they are doing in the app.

If you turn analytics back on we will check the status of your account and update it, so that you only get reminders that are relevant to actions you then take in the app. For example, if you turn off analytics and then add a document, we will not know that you have added a document so you would not get any document-related reminders. If after adding the document you turn the analytics back on, we will update your account status to show that there is a document. You would then get any reminders that are relevant to users who have added documents.

Past versions

We changed how we present our privacy information in January 2019 to distinguish between general information and product-specific information. You can find previous versions of the entire privacy information under the ‘Past versions’ heading in the ‘General’ section. We will add here past versions of the Yoti app privacy information if it has been updated.

14 January 2019
4 March 2019
27 May 2019
22 July 2019
19 August 2019
16 September 2019
16 December 2019
30 March 2020
27 April 2020

What’s new

- We have added information about the different ways an organisation can issue a test result or other credential into your Yoti. (Section: Information collection and use > Adding information from third parties)

- We have added to our information on biometrics to reflect the fact we now use different technologies to check you are a real person. We have also added some heading sections to better organise the information. (Section: Biometrics)
- We have clarified that for the purposes of the California privacy law, we do not sell your information. We have also added a link to a list of global regulators so you can easily find your local one. (Section: Your rights and choices)