

Citas

Privacy Policy

Welcome to the Citas Privacy Policy (“Policy”)! This explains how we collect, store, protect, and share your information, and with whom we share it. We suggest you read this in conjunction with our Terms and Conditions of Use.

Whilst you’re enjoying the Citas mobile application (including the desktop version) (“App”), our websites and microsites (such as citashub.com) using our digital products and services (such as our competitions or surveys) (together, referred to in this Privacy Policy as our “Sites”), we collect some information about you. In addition, you may choose to use the App or Sites to share information with other users, including your friends and contacts (“Users”). We may also need to share your information sometimes.

The App and Sites are global, and your information will be sent to and used in the country you reside in. This Policy explains how we protect your personal data when we transfer it overseas, so please read very carefully!

Who we are

The App and Sites are operated by the “Citas Group” (also referred to in this policy as “we” or “us”) which includes Citas Holding Limited, Turtl Cyber Security Industry and Development Pvt Ltd, all of which are controllers of personal information collected and processed through the citas App and Sites.

The Citas Group has designated a Data Protection Officer and they can be reached by emailing service@turtltech.com or by post at the following address: B-25 first floor Noida sector-1 Up INDIA

1. COLLECTION OF INFORMATION.

Registration Information

When you download the App and create an account (“Account”), we may collect certain information (“Registration Information”) about you, such as:

Name;

Email address;

Cell number;

Gender identity;

Date, time, and location of birth;

Sexual preference;

Photographs;

Location; and

Login information for social media accounts that you connect to your citas Account (this could include, for example, your Facebook, Instagram accounts, Gmail. etc). For more information about this, see “Linking other Accounts to citas” in section 7 below.

Once you register, you will be able to review and change this information at any time just by logging in to citas (other than your date of birth and location (which, if you have given citas access to your location in your device settings, is automatically updated based on the location of your device)). It is your responsibility to ensure that your account details are kept up to date. If your phone number changes, please ensure that you update this in your account.

The information we collect helps to enhance the App and verify our Users (robots are not welcome!). Registration Information such as your sexual preference, name, and username may be visible to other Users who view your profile page.

For Users who are INDIA residents, the data we may collect falls within the following categories of “personal information”, as defined by the INDIAN Privacy Act:

A. Identifiers, such as name and location;

B. Personal information, as defined in the INDIAN records law, such as contact (including email and telephone number) and financial information;

C. Characteristics of protected classifications under California or federal law (if you choose to provide them), such as age, gender identity, marital status, sexual orientation, race, ancestry, national origin, religion, and medical conditions;

D. Commercial information, such as transaction information and purchase history;

E. Biometric information;

F. Internet or network activity information, such as browsing history and interactions with our Sites and App;

G. Geolocation data, such as mobile device location;

H. Audio, electronic, visual, and similar information, such as photos and videos;

I. Professional or employment-related information, such as work history and prior employer;

J. Non-public education information; and

K. Inferences are drawn from any of the personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

Profile Information

We recommend and encourage you (and all our members) to think carefully about the information you disclose about yourself. We also do not recommend that you put email addresses, URLs, instant messaging details, phone numbers, full names or addresses, credit card details, national identity numbers, driver's license details, and other sensitive information that is open to abuse and misuse on your profile.

When you post information about yourself or use the messaging function to communicate with other Users, the amount of personal information you share is at your own risk. Please see Section 4 below for more information on who can access what you post on CITAS.

Profile Verification Information (Including Biometric Information)

For safety and security and to ensure you have the best possible user experience, we require Users to verify their accounts and ask for your phone number, and, in some instances, we might also ask that you carry out photo verification. We want to make sure you are not a robot! We also want to avoid fake CITAS accounts being created which can be used for malicious activities and cybercrime – they threaten the CITAS Network and spoil things for everyone. This verification might be required by us for the prevention of fraud. You can also verify your photo voluntarily (to add the blue 'verified' badge to your profile).

If you choose to verify your profile photo, we will scan each photo that you submit. The scan may include the use of facial recognition technology so that we can compare the photo you submit to your profile photo, to help ensure that you are who you say you are. We do not add the verification photos to your profile. We retain the scans so that we can verify you in the future and for our record-keeping purposes until we no longer need them for such purposes or for three years after your last interaction

with us, whichever occurs first. After the applicable retention period expires, we take commercially reasonable steps to permanently and securely delete the scans from our systems.

Purchases Information

If you decide to purchase any of our premium services, we will process your payment information and retain this securely for the prevention of fraud and audit/tax purposes.

Please note that if your account is blocked for any reason, any account(s) that you have on other CITAS Group platforms/applications, may also be blocked as part of our anti-spam and anti-fraud procedures.

Geolocation Information

If you have given CITAS access to your location in your device settings, when you use your cell, we will collect information about WiFi access points as well as other location information about your longitude and latitude and may save your device's coordinates to offer certain features to you. This information helps us identify your physical location and we use it to personalize the App and make it easier for you to interact with other Users, by enabling the general locality information to be displayed to Users seeing your profile and showing you the profiles of other Users who are near you.

If you have given CITAS access to your location, but wish to turn this off, you can do so by the following methods:

iPhone app — settings, privacy, location services, citas

Android — settings, location, citas, permissions, location

Device and Photos Information

We may collect information about your device when you use the App including the unique device identifier, device model, and operating system, for several purposes, as set out in this policy. In addition, if you permit us to do so, the App may access your device's address book solely to add someone to your contacts.

We also collect data about your photos, such as which are the photos that users spend time on or which are the photos that have the best lighting, etc. We may use that data to rearrange your profile photos aiming to position them in a way that is favorable to you. You may opt out of this feature through our app settings.

Links

We may keep track of how you interact with links available on citas including third-party services by redirecting clicks or through other means. We may share aggregate click statistics such as how many times a particular link was clicked on.

Messages

We review the content of messages sent in the App to identify topics, sentiments, and trends across our Users. We will take steps to remove personally identifying information from such messages, prior to reviewing them. We will not share the content of User messages or information we derive from them with any third party.

When you Contact Customer Support

If you contact our Customer Support team via our Feedback Page, we will receive your email address, and may track your IP address, as well as the information you send to us to help resolve your query. We will keep records of our communications with you, including any complaints that we receive from you about other Users (and from other Users about you) for 10 years after deletion of your account.

Cookies and similar technologies

When you visit our Sites or when you use our App, we may collect personal data from you automatically by using cookies or similar technologies. A cookie is a small file that can be placed on your device or browser that allows us to recognize and remember you.

If you would like to find out more about cookies, including how we use them and what choices are available to you, please refer to our Cookie Policy.

2. USE OF YOUR INFORMATION.

Our main goal is to ensure your experience on citas is an enjoyable one and you don't end up getting stung! In order to deliver an enjoyable experience to you, we may use your Registration and other information to:

offer you our services and features;

contact you with information about the App (e.g., updates and new features);

personalize the App/Sites and the content we deliver to you;

conduct research and analytics about how you use and interact with the App/Sites;

to test new technologies and processes designed to enhance and improve the App/Sites;

resolve disputes, troubleshoot problems and to enforce our Terms & Conditions;

investigate fraud, protect our legal rights, and to enforce our Terms & Conditions.

to send you information about the promotions and offers we have available (e.g., specify the types of goods/services/offers to be provided via direct marketing) by direct marketing or other modes of communication - if you've signed up for our communications or otherwise told us it's OK. We will not use your information in email direct marketing unless you give us your consent during the Account creating process or via Settings in the App (you can withdraw from marketing at any time via Settings in the App or by using the opt-out mechanisms and links provided in each message); and

protect our Users and third parties from harm.

Our Matching Algorithms

CITAS mission is to create kind and equitable relationships. We have developed matching algorithms to predict your compatibility with other users so we can show you people we think are a good match for you. We use different indications based on users' profiles on our app (for example, how you swipe or whether you match with someone). We use these indications to recommend the most relevant profiles to everyone to maximize everyone's chances of finding meaningful connections on our apps. Our matching algorithms are based on a range of factors and use machine learning to rank profiles for you to maximize your chance of finding compatible matches. We use the following data about you and other users to predict your compatibility with others and generate profile recommendations: the information you provide us about yourself in your profile such as age, distance or gender so we can show you people who are appropriate and are more likely to like you back; information about how you interact with our app to suggest to you people who are active and available to meet new people; and your device coordinates, which are necessary to understand your proximity to other members. The legal basis for processing profile and proximity information is that this is necessary for the provision of our contractual services to you pursuant to Article 6(1)(b) GDPR. Where we process information about your app activity, this is based on our legitimate interests pursuant to Article 6(1)(f) GDPR, and specifically our legitimate

interest in generating more personalized and relevant recommendations for who you can match with in our App. Where you have included sensitive information in your profile, such as information about your beliefs, the processing of this information is based on your voluntary and explicit consent.

Moderation Practices

We use a combination of automated systems and a team of moderators to monitor and review accounts (including photos and any other information uploaded onto user profiles) and messages for content that indicates breaches of our Terms and Conditions of Use. If an account or message meets certain criteria that demonstrate that the Terms and Conditions of Use are likely to have been breached, the relevant account will be subject to a warning and the user's access restricted and/or blocked. Affected Users can contact citas to contest the decision.

If you post anything that is inconsistent with our Terms and Conditions of Use, we reserve the right to terminate or restrict access to your Account.

Lawful Basis

Under India data protection laws, we are required to tell you our lawful basis for using your data and we have set this out in the table below. Where the legal basis is consent, you can withdraw consent at any time. Where the legal basis is legitimate interests, you have a right to object to our use of your data. We explain in the relevant sections in this Policy how you can withdraw consent or opt-out of certain data uses (where applicable).

Purpose for which data is used	Data	Source	Legal basis
--------------------------------	------	--------	-------------

To provide you with the CITAS social networking service	Name, email address, date of birth, location (CCPA Categories A and B)	You provide your name, email address and date of birth to us. We obtain location data from the device that you use to access the service	Contractual necessity
---	--	--	-----------------------

To facilitate networking opportunities on the citas App	Optional information that you choose to provide in your profile, including through profile verification, or adding citas badges, which may include information about your sexual preferences, non-binary gender, religion, ethnic background, photos, interests, etc. (CCPA Categories B, C, H, I, J)	You provide this information to us	Contractual necessity and our legitimate interests – it is in our legitimate interests to facilitate networking opportunities in the citas app. For special category/sensitive personal data, we rely on your explicit consent.
---	---	------------------------------------	---

To verify your identity and prevent fraud and to ensure the safety and security of Users	Phone number and if requested or permitted, photo provided as part of profile verification and for users based in countries where age verification is required by law: photo of Government ID + geolocation and device information (CCPA Categories A, B, C, E, F, G and H)	You provide this information to us, except for	
--	---	--	--

the geolocation and device information, which we obtain from the device that you use to access the service Legitimate interests – it is in our legitimate interests to ensure that accounts are not set up fraudulently and to safeguard Users of the site

To take payment for premium services (not applicable for Users making payments via the Apple App Store) Payment card details (CCPA Categories B and D) You provide this information to us

Contractual necessity

To send you marketing information about our events, offers and service Name, email address, postal address, Instagram handle and mobile phone number (CCPA Categories A and B) You provide this information to us Consent or legitimate interests and in accordance with the laws applying to our marketing activities. We have a legitimate interest in promoting our business and products

To carry out research and analysis to help us improve the App and to test new technologies and processes designed to enhance and improve the App/Sites Log and usage data, including IP address, browser type, referring domain, pages accessed, mobile carrier and search terms, images and video, registration information, profile information (CCPA Categories A, F and H) You provide photos and videos to us. We obtain the log and usage information from the device that you use to access the service Legitimate interests – it is in our legitimate interests to analyze the way in which Users are accessing and using our services and to test new technologies so that we can further develop the App, implement security measures and improve the service

To respond to correspondence and queries that you submit to us, including social media queries Email address and IP address, social media name, phone number (CCPA Categories B and F) You provide your email address, social media name and phone number to us when you contact us and we obtain your IP address from the device that you use to contact us Legitimate interests – it is in our legitimate interests to respond to your queries to ensure that we provide a good service to Users and troubleshoot problems

To investigate and block Users for reported infringements of our Terms and Conditions of Use Name and user registration details, profile information, content of messages and photographs + usage and device data such as IP address and IP session information (CCPA Categories A, B, C, F, and H) You provide your registration details, profile information, messages and photographs to us. We obtain the other information from the device that you use to access the service. Legitimate interests - it is in our legitimate interests to prevent unauthorized behavior and to maintain the safety and integrity of our services

To improve your experience on the App Data about profile photos such as whether the first profile photo is scrolled on or not and whether the vote is a yes or a no We obtain this information from the way users interact with the App and the profile photos of other users Legitimate interest - it is in our legitimate interest to improve our users' experience

To enable Users to create and enhance their CITAS profile and log into the App via third-party accounts Data from Facebook and other third-party accounts (see section 7 of this Privacy Policy for more details)

(CCPA Categories A, B, C, and H) We obtain this information from Facebook, or the providers of any other accounts you use to log in or connect with your CITAS account Legitimate interests – it is in our legitimate interests to facilitate access to our services

To block payment transactions as part of our anti-fraud procedures Name, IP address, email address, mobile number, cardholder name, payments received, type of payment, user ID, and country (CCPA Categories, A, B, and D) You provide your name, email address, mobile number and card details to us. We obtain your IP address from the device that you use to contact us. We obtain your payment information from your interactions with our service Legitimate interests – it is in our legitimate interests to prevent fraudulent transactions and to maintain the security of our services

To serve promo cards and advertisements on the App Location, gender, age, and information that you have optionally provided us with via your profile (CCPA Categories A, C, and G) We obtain age, gender, and profile information from you, and location data from the device that you use to access the service Legitimate interests – it is in our legitimate interests to target advertisements so that Users see relevant advertisements and to allow us to generate income from advertising revenue

To serve advertisements on third-party networks and measure the effectiveness of such ads Data about your visit to our Sites or App and action taken on those (for example if you downloaded our App or created an account with Citas), IP address (and your estimated location based on your IP address), age and gender, device ID (CCPA Categories B, C, G, F and K) We obtain age and gender from you and we obtain other information from the device or browser that you use to access the service Consent – as indicated by you in your Privacy Settings/Cookies Settings preferences and via your browser or device privacy preferences (where required by your device manufacturer, for example, Apple devices using iOS 14.5).

To contact you to run surveys for research purposes to obtain feedback, and to find out if you want to take part in marketing campaigns Email address and cell phone number (CCPA Category B) You provide this information to us Legitimate interests – it is in our legitimate interests to research so that we can further develop the app and improve the service

To enable video and audio call functions, and the sending of images and video audio call usage data, images, and video (CCPA Categories F and H) We obtain this information from the device that you use to access the service Legitimate interests – it is in our legitimate interests to provide these functionalities as part of the services

To defend legal claims, protect legal rights, and protect people from harm This could include any information that is relevant to the issue This information may be obtained directly from you, from your device or from third parties, depending on the information involved Legitimate interests – it is in our legitimate interests to protect our legal rights, defend legal claims and to protect our Users and third parties from harm

Processing We Perform To Improve Services For Students

What we're doing. We process personal data to understand which of our users may be in college or university. To do this, we look at historic location data to understand whether your device's coordinates match to a general university or college area. For this activity, we use recent historical data regarding where you opened the citas app and we'll keep a simple "at campus yes/no" result based on our

findings. What we don't do. We do not track your real-time movements as part of this activity and we do not identify or store information about where you are studying. To protect your privacy, we do not retain any of the location data used for this activity and it is permanently deleted once the results are generated. Why we're doing this? We'll combine the results of this processing with other relevant information we hold for the following purposes: so we can send the right offers, events, and features to the right users; to understand which citas events are popular with the student demographic and which aren't working so well; and to improve the design of the App to meet the needs of students. The legal basis for this processing is our legitimate interests. We have a legitimate interest in providing a more tailored app experience for student users and in optimizing their chances of finding the right connections. Please note this processing only affects citas App users who identified the United States or Canada as their location when registering for the App (we exclude users in Quebec) and who are in the 18 to 24 age group.

3. DISCLOSURE OF INFORMATION.

Our policy is to not disclose your Registration Information or personal data, except in the limited circumstances described here:

Circumstances where data may be disclosed	Disclosed data
---	----------------

Service Providers – We engage certain trusted third parties to perform functions and provide services to us. We may share your Registration Information or personal data with these third parties, but only to perform these functions and provide such services. More information about this is available directly below. This could include all data, including all CCPA Categories listed above	
--	--

Moderators – To monitor activity on the App and approve content. Name and user registration details, profile information, content of messages and photographs (CCPA Categories A, B, C, and H)	
--	--

Payment Processing and Telecommunications Companies – To facilitate payments for our premium services. Cardholder name, cardholder address, card number, payment amount, transaction date/time (CCPA Categories A, B, and D)	
--	--

Law and Harm – As we mentioned in the Terms & Conditions, we think it is very important that all Users behave whilst using the App. We will cooperate with all third parties to enforce their intellectual property or other rights. We will cooperate with lawfully made law enforcement requests for information from within or outside your country of residence where we are required to by law. This may include where there is an investigation into alleged criminal behavior or to protect the vital interests of a person. We may preserve or disclose any of your information, including your Registration Information, if we believe in good faith that it is necessary to comply with a law or regulation, or when we believe in good faith that disclosure is necessary:	
---	--

to comply with a binding direction court order, or lawful request;	
--	--

to protect the safety of any person;	
--------------------------------------	--

to address fraud, security or technical issues e.g. through anti-spam providers to protect the service from criminal activity; or

to protect our rights or property or those of third parties.

In such cases, we may raise or waive any legal objection or right available to us. This could include any personal data that citas holds about you, depending on the nature of the request or the issue that we are dealing with, including all CCPA Categories listed above

Business Transfers – If a citas Group entity or any of its affiliates undergoes a business transition or change of ownership, such as a merger, acquisition by another company, reorganization, or sale of all or a portion of its assets, or in the event of insolvency or administration, we may be required to disclose your data. This could include all personal data that citas holds about you, including all CCPA Categories listed above

Marketing Services Providers – To help us serve marketing and advertising on third-party websites and applications and measure the effectiveness of our advertising campaigns. More information on this is available below Advertising identifier associated with your device (Device ID), estimated location (based on your IP address), age, gender, and data about your visit to our Sites or App and action taken on those (for example if you downloaded our App or created an account with our App), hashed email address (for ‘custom audiences’ only) (CCPA Categories B, C, G, F and K)

Anti-Spam and Anti-Fraud – Your data may be shared with other citas Group companies, for example, to block accounts and suspected fraudulent payment transactions as part of our anti-spam and anti-fraud procedures. Email address, phone number, IP address and IP session information, social network ID, username, user agent string, and transaction and payment data (CCPA Categories B, F, and D).

Aggregated Information – We may share aggregated information with third parties that includes your data (but which doesn’t identify you directly) together with other information including log data for industry analysis and demographic profiling.

MORE INFORMATION ABOUT DISCLOSURES

Service Providers

We engage certain trusted third parties to perform functions and provide services to us (“Service Providers”). The suppliers with which citas share User personal data vary depending on a variety of factors, such as which of our Apps, Sites, and services a User engages with. For example, to provide our services to Users, we typically use the following suppliers:

Billing services – to allow customers to purchase paid features of our App (for example, Google Play)

Authentication services – to allow customers to authenticate their account (for example, Twilio)

Social media providers – to allow customers to create/connect their Citas account with their account(s) on such platforms (for example Facebook, Instagram or Spotify)

Product improvement and market research – we use third-party platforms (such as Typeform) and agencies (such as Kantar) to carry out customer surveys and market research to improve our products and services

IT services – some of the third-party software providers used in the operation of our business may process Users' data (for example, if a User contacts us via social media with a support inquiry, their inquiry is processed by our community management software provider Khoros)

We carry out due diligence on all Service Providers we engage to ensure they have adequate data protection and information security measures in place and only provide them with the personal data necessary for the service they are providing. Measures are taken to ensure that the data shared is non-attributable to the greatest extent possible and our suppliers are also subject to extensive obligations under our contractual arrangements, including strict data retention limits.

Marketing Services Providers

We partner with providers of marketing services (such as Facebook for example) ('Marketing Services Providers') to help us market and advertise our App and services on third-party websites and applications and measure the effectiveness of our advertising campaigns. For example:

to exclude you from advertising campaigns aimed at finding new users, if you already have a Citas account;

to show Citas adverts to users who have visited the Citas app/Sites but haven't yet created a Citas account;

to create an audience for our advertisements of other potential users who have similar characteristics to you based on the information the Marketing Service Providers hold about you (also known as a Lookalike Audience); or

to include you in a 'custom audience' that will receive Citas advertising content (a custom audience is essentially a list of people who we think are most likely to be interested in a particular advertisement).

We share a limited amount of your data with these Marketing Services Providers, such as:

the advertising identifier associated with your device (this is a random number assigned by your mobile device manufacturer (for example Apple or Google) to your device to help advertisers (including the manufacturer) know when an ad has been viewed or clicked in an app, and when an ad causes a 'conversion' (for example, downloading the app advertised to you))

your estimated location (based on your IP address)

Age and Gender

data about your visit to our Sites or App and action taken on those (for example if you downloaded our App, created an account with our App, or details of any purchases made on Site or in App)

a hashed* version of your email address (to create 'custom audiences').

*Hashing is a way of encrypting information by turning it into a combination of random numbers and letters - this code cannot be traced back to the email address. When hashed email addresses are sent to a Marketing Service Provider, they're then matched against the Provider's existing list of their own users' hashed information, and our ads are served to those of our users who have successfully been matched with the Provider's. Matched and unmatched hashes are then deleted by the Provider.

For more information about how we use cookies and other tracking technologies, including how you can set and manage your preferences about such technologies, please see our Cookie Policy.

In some cases, these third parties will also use the data that they collect for their purposes, for example, they may aggregate your data with other data they hold and use this to inform advertising-related services provided to other clients.

Facebook

Where we share data with Facebook as our Marketing Service Provider (including via the Facebook "Like" function), we are Joint Data Controllers with Facebook Ireland for this processing. This arrangement means that citas has to provide you this notice, but you should contact Facebook if you wish to exercise your data protection rights. Further information, including how Facebook enables you to exercise your data protection rights and subsequently processes your information as an independent data controller can be found in Facebook Ireland's Data Policy. If you want more information relating to the nature of the arrangement we have in place with Facebook, please email DPO@citas.com.

This data referred to above can include actions that you take on our website such as your interactions with our Sites or other information collected from cookies or similar technologies including the Facebook pixel. This allows us to measure the effectiveness of our advertising, improve our marketing practices, and help us deliver more relevant advertising to you and people like you (including on social media such as Facebook).

4. WHAT OTHERS MAY SEE ABOUT YOU.

We think our Users are awesome, and we want you to share how awesome you are with the world, so we have built certain features to enable this. Our App is designed to make it easier for you to connect with other Users and to interact with them.

When using the Citas app, you should assume that anything you post or submit on the App may be publicly viewable and accessible, both by Users and non-users of the App. We want our Users to be careful about posting information that may eventually be made public.

Please be careful about posting sensitive details about yourself on your profile such as your religious denomination and health details. You may also choose to add sensitive information about yourself when you add certain citas badges to your profile, such as your religion and political leanings. While you may voluntarily provide this information to us when you create your profile, including your sexual preferences, there is no requirement to do so. Please remember that photographs that you post on citas may reveal information about yourself as well. Where you do upload and choose to tell us sensitive information about yourself, including through the addition of badges to your profile, you are explicitly consenting to our processing of this information and making it public to other Users.

Your citas profile and other information you make available via the App, including certain information added to your profile through third-party accounts (such as Facebook, Instagram, or Spotify – see section 7 of this Privacy Policy for more information about this) may be viewed and shared by Users with individuals who may or may not be users of the App. For example, a User may recommend you as a match to his or her Facebook friend(s) by taking a screenshot of your profile picture and sharing it, regardless of whether such friend(s) is also a User of the App.

Please also note that in certain countries (currently, South Korea only), Users are provided with functionality enabling them to download a copy of their conversation history (as this is required by local laws) and that citas has no control over how users may then publish or use that information.

If you log in to or access the App through your Facebook account or another third-party account on a device that you share with others, remember to log out of the App and the relevant third-party account when you leave the device to prevent other users from accessing your citas account.

5. OUR POLICY TOWARDS AGE.

Although we want as many people as possible to enjoy our creation, you have to be at least 18 years old to use citas.

citas does not knowingly collect any information about or market to children, minors or anyone under the age of 18. If we become aware that a child, minor or anyone under the age of 18 has registered with us and provided us with personal information, we will take steps to terminate that person's registration.

6. SECURITY.

Here at citas, we pride ourselves on taking all appropriate security measures to help protect your information against loss, misuse and unauthorized access, or disclosure. We use reasonable security measures to safeguard the confidentiality of your personal information such as secured servers using firewalls.

Unfortunately, no website or Internet transmission is ever completely 100% secure and even we cannot guarantee that unauthorized access, hacking, data loss or other breaches will never occur, but here are some handy tips to help keep your data secure:

Please make sure you log out of your Account after use as you never know who may stumble onto your Account!

Please don't share the password you use to access your citas Account with anyone else!

Change your password periodically.

If you ever think someone has had access to your password or Account, please follow the steps set out here. We cannot guarantee the security of your personal data while it is being transmitted to our site and any transmission is at your own risk.

7. LINKING OTHER ACCOUNTS TO Citas.

Using your social media details to sign in to citas

When you sign in to our App using your Facebook account, you give permission to Facebook to share with us your name and profile picture. Unless you opt-out, you also give permission to Facebook to share with us your email address (if there is one associated with your Facebook account), date of birth, profile photos, gender, Page likes and current town/city.

If you register or sign in with your Apple ID, you give Apple permission to share your Apple login, a name (that can be edited by you) and an email (you can choose to hide your email and Apple will create a random email address so your personal email can stay private). This email address will be linked to your citas account and will be used to retrieve your citas account.

We will then use this personal data to form your citas account. If you remove the citas app from your Facebook settings, or from your Apple ID, we will no longer have access to this data. However, we will still have the personal data that we received when you first set up your citas account using your Facebook or Apple ID (you must delete your citas account entirely for us to no longer have access to this data).

Linking social media accounts to your citas account

You may link your citas account with your Instagram, Facebook or Spotify accounts. This allows you to share some information from those accounts directly to your citas account (for example, Instagram photos, or your top Spotify artists).

We only receive the limited information that Instagram or Spotify permits to be transferred (as detailed by Instagram/Facebook/Spotify and agreed by you when you first connect your account from such platforms with your citas account).

If you no longer want to link your citas account to your Instagram, Facebook or Spotify account, please visit the settings in your Instagram, Facebook or Spotify account and follow the instructions to remove the citas app access permissions. Please note that any information already added to your citas account from those platforms will not be deleted unless you delete it within your citas account as well.

8. INFORMATION FOR BFF MEMBERS.

If you use BFF, you can populate your profile with information (like your beliefs and political leanings). You can provide this information as part of your profile, but there's no obligation to do so.

You should assume that whatever information you share in BFF, including which Hives you've joined, can be seen by any BFF member. Please note BFF members will not be able to see chat discussions until they join the specific chat and when they join, they'll see the full chat history.

How we process personal data in BFF and our legal bases for processing

We offer the opportunity in BFF to join Hives built around locations or topics. We'll automatically recommend Hives you can join based on your location, activity, "my life" and "my interests" information.

The processing of your location data is necessary in order to perform our contract with you and deliver the Hives service to you.

The processing of your profile and activity information in order to make Hive recommendations is based on our legitimate interests. It is in our legitimate interests to use this information to recommend relevant Hives to you.

Please note that if you upload and choose to share sensitive information (such as sexuality and beliefs), you are explicitly consenting to sharing that information with other BFF members.

Profile Sharing on Our citas For Friends App

If you are a member of BFF, your BFF profile will automatically be visible both on BFF mode in citas and on our separate app, citas For Friends. citas For Friends is a separate app for finding friendship and is owned by citas Group. We automatically show BFF profiles both on BFF mode in citas and on our citas For Friends app to provide you with a richer pool of potential friends to connect with. Please note that this profile sharing only applies to BFF members in the jurisdictions where our citas For Friends app is available. If you object to your BFF profile being shown on our citas For Friends app, please see this help page.

9. YOUR CALIFORNIA PRIVACY RIGHTS.

For Users who are California residents, you have the following rights (in addition to those listed at section 10 below) under the California Consumer Privacy Act, and you have the right to be free from unlawful discrimination for exercising your rights under the Act:

You have the right to request that we disclose certain information to you and explain how we have collected, used and shared your personal information over the past 12 months.

You have the right to request that we delete your personal information that we collected from you, subject to certain exceptions.

California's "Shine the Light" law, Civil Code section 1798.83, requires certain businesses to respond to requests from California customers asking about the businesses' practices related to disclosing personal information to third parties for the third parties' direct marketing purposes. If you wish to find out about any rights you may have under California Civil Code section 1798.83, you can write to us at feedback@team.citas.com.

From time to time, as part of a joint promotion with a third party, we may, if you participate in such promotion, disclose your contact information to the third party to allow them to market their products or services to you. Where this is a condition for participation in a promotion, we will always let you

know before when you enter the promotion. Please follow the instructions provided to you by third parties to unsubscribe from their messages.

In addition, under California law, operators of online services are required to disclose how they respond to “do not track” signals or other similar mechanisms that provide consumers the ability to exercise choice regarding the collection of personal information of a consumer over time and across third party online services, to the extent the operator engages in that collection. At this time, we do not track our Users’ personal information over time and across third-party online services. This law also requires operators of online services to disclose whether third parties may collect personal information about their users’ online activities over time and across different online services when the users use the operator’s service. We do not knowingly permit third parties to collect personal information about an individual User’s online activities over time and across different online services when using the App.

10. YOUR RIGHTS.

Privacy laws applicable in your country may give you the following rights:

Right to be informed: what personal data an organization is processing and why (we provide this information to you in this Privacy Policy).

Right of access: you can request a copy of your data.

Right of rectification: if the data held is inaccurate, you have the right to have it corrected.

Right to erasure: you have the right to have your data deleted in certain circumstances.

Right to restrict processing: in limited circumstances, you have the right to request that processing is stopped but the data retained.

Right to data portability: you can request a copy of certain data in a machine-readable form that can be transferred to another provider.

Right to object: in certain circumstances (including where data is processed on the basis of legitimate interests or for the purposes of marketing) you may object to that processing.

Rights related to automated decision-making including profiling: there are several rights in this area where processing carried out on a solely automated basis results in a decision which has legal or significant effects for the individual. In these circumstances your rights include the right to ensure that there is human intervention in the decision-making process.

The particular rights which are applicable to you (which might include other rights not listed above) may vary depending on your country. You should make yourself aware of the rights you have under applicable privacy laws in your country.

If you want to exercise any of your rights listed above please visit our Feedback Page or email our Data Protection Officer at DPO@citas.com. You can also contact us by post at the following address: The Broadgate Tower Third Floor, 20 Primrose Street, London, United Kingdom, EC2A 2RS. For your protection and the protection of all of our Users, we may need to request specific information from you to help us confirm your identity before we can answer the above requests.

If you have a concern about how we have processed your request or your personal data, you should contact us in the first instance via the contact details listed above.

If you feel we have not resolved your concern, 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. If you live in a country or territory located in the European Union (EU) or European Economic Area (EEA), you may also get in touch with your local Data Protection Regulator. If you live in a country outside the EU, you may have the right to lodge a complaint with your local privacy or data protection regulator.

EU Representative

Pursuant to Article 27 of the General Data Protection Regulation (GDPR), citas has appointed Borlux Ltd as its GDPR representative in the EU. If you usually reside in an EU Member State you can contact Borlux Ltd regarding matters pertaining to the GDPR by:

Using the online request form at <https://services.nathantrust.com/privacycontact>

Postal address: 1st Floor, 6 Lapps Quay, Cork, Ireland

11. DATA LOCATIONS.

We want you to be able to access citas wherever you happen to be in the world. To enable us to provide that service, we operate a global network of servers including in the US, UK, EU, and (for Users located in Russia) Russia. The hardware is located in third-party data centers but is owned by the citas Group. Data collected by Advertising Partners and other Service Providers may also be held outside the UK and the European Economic Area. We ensure that the data is adequately protected by ensuring that valid, legal mechanisms are in place such as: EU approved model clauses, and implementing robust contractual standards. If you want more information relating to the nature of the safeguards we have in place, please email DPO@citas.com.

12. DATA RETENTION AND DELETION.

We keep your personal information only as long as we need it for the legal basis relied upon (as set out in Section 2 above) and as permitted by applicable law. Please see “Profile Verification Information (Including Biometric Information)” in Section 1, above, to learn about our retention policy with respect to biometric information.

When your Account is deleted, we make sure it is no longer viewable in the App. For up to 28 days, it is still possible to restore your Account if it was accidentally deleted. After 28 days, we begin the process of deleting your personal information from our systems, unless:

we must keep it to comply with applicable law (for instance, if you make purchases within the App, some personal data may be kept for tax and accounting purposes);

we must keep it to evidence our compliance with applicable law (for example, if an account is blocked, we keep some account information and a record of the behavior that led to the block - this information is retained for evidential purposes in case of queries or legal claims concerning the block);

there is an outstanding issue, claim or dispute requiring us to keep the relevant information until it is resolved; or

the information must be kept for our legitimate business interests, such as fraud prevention and enhancing Users’ safety and security (for example, information may need to be kept to prevent a user who was banned for unsafe behavior or security incidents from opening a new account).

Warning: Even after you remove information from your profile or delete your Account, copies of that information may still be viewable and/or accessed to the extent such information has been previously shared with others, or copied or stored by others. We cannot control this, nor do we accept any liability for this. If you have given third party applications or websites access to your personal information, they may retain such information to the extent permitted under their terms of service or privacy policies.

Thanks for reading, we hope we didn’t drone on for too long!

13. CHANGES TO THIS POLICY.

As citas evolves, we may revise this Privacy Policy from time to time. The most current version of the policy will govern our use of your information and will always be at citas.com/privacy. If we make a change to this policy that, in our sole discretion, is material, we will notify you, for example, via an email to the email associated with your Account or by posting a notice within citas.

Effective date

This Privacy Policy was last updated on: February 16th 2024