

Privacy Policy for Serus AI

Last updated: **October 26, 2026**

1. Introduction

Serus AI ("the App", "we", "us", "our") is an iOS application that helps you find where your personal information has been exposed in data breaches and on people-search websites, and helps you request its removal.

Because this App exists to protect your privacy, we hold ourselves to a strict standard: we collect only what a specific feature genuinely requires, we do not sell your personal information, and we do not use it for advertising.

This policy explains what we collect, why, who we share it with, and what control you have over it.

Contact us: support@decentsoftwares.in

2. Your Account Is Anonymous by Default

Serus AI does not require you to create an account, provide an email address, or set a password in order to use it.

When you first open the App, we create an anonymous account identifier — a random ID issued by Firebase Authentication. This ID is what links your scans and removal requests to you. It is not tied to your name, your Apple ID, your email address, or your real identity, and we cannot use it to work out who you are.

Please understand one consequence of this. Because the account is anonymous and its session lives only on your device, deleting the App loses that identifier permanently. Reinstalling creates a brand-new one, and your previous scan history and removal reports will no longer be reachable — by you, or by us in any way we can connect back to you. Your subscription can be restored through the App Store, but your history cannot.

3. Information We Collect

3.1 Information you give us

Email address — collected when you run an email breach scan, and used to check that address against known data-breach records.

Phone number — collected when you run a reverse phone lookup or set up a site sweep, and used to identify records published about you.

Password — collected when you use the free Password Checker. As explained in Section 4, your password never leaves your device and is never stored by us or by anyone else.

Name and address details — your full name, current address, previous addresses, postal code, country, city, state, and approximate age. These are collected when you submit a removal request or set up a site sweep, and are used to file opt-out and deletion requests on your behalf. The sites receiving those requests require these details in order to locate and verify your records.

Photo identification — collected only where a particular data broker requires proof of identity before it will honor a deletion request, and used only for that verification.

Support correspondence — anything you send us when you contact support, used to answer your question.

3.2 Information returned about you by search services

When you run a reverse phone lookup or a site sweep, the App queries people-search and data-broker sources on your behalf. Those sources may return a profile about you containing your full name and approximate age, your current and previous postal addresses, other phone numbers associated with you, email addresses associated with you, the names of relatives or associated people, and links to public listings about you.

We did not create this information and we are not its source. It is already published by third-party data brokers. The App retrieves it so that you can see what is exposed and act on it. It is saved to your scan history so that you can reopen a past result without running the search again.

When you run an email breach scan, we receive and store the breach records matching that address: the name of the breached service, its domain, the date of the breach, how many accounts were affected, and which categories of data were exposed.

3.3 Information collected automatically

We store a push notification token alongside your anonymous account, so that we can tell you when a removal has been filed or a report is ready. Notification permission is requested in context rather than at launch, and you can decline it or revoke it in iOS Settings at any time.

We also record whether you hold an active premium subscription, and we send the app version and platform with requests for compatibility and support purposes.

A small number of preferences stay on your device only and are never transmitted to us: whether you have completed onboarding, how many times you have opened the App, and the timing used to pace the App Store review prompt.

3.4 What we do not collect

We want to be specific here, because vague privacy policies are how this problem started.

We do not access your contacts. We do not collect your location or use location services. We do not collect an advertising identifier and we do not include any advertising SDK. We do not track you across other apps or websites. We do not sell or rent your personal information to anyone. We do not require your real name to use the App's scanning features.

4. Password Checking: Your Password Never Leaves Your Device

The free Password Checker uses a technique called k-anonymity. We want you to understand exactly how it works, because you should never have to simply trust an app with a password.

First, your password is hashed on your device using SHA-1. Second, only the first five characters of that hash are sent to the Have I Been Pwned "Pwned Passwords" service. Third, that service returns every hash suffix that begins with those five characters — hundreds of them. Fourth, your device compares them locally and tells you whether yours is among them.

The password itself, and its full hash, never leave your phone. The service cannot determine which password you checked. We additionally request response padding, so that even the size of the reply gives nothing away.

Password checks are never saved to your history and are never stored on our servers.

5. How We Use Your Information

We use the information described above only to run the scans, lookups and sweeps you request; to show you your scan history and removal reports; to submit opt-out and deletion requests to data brokers, people-search sites and breached services on your behalf; to notify you about the progress of those requests; to manage your subscription and unlock premium features; to respond to your support requests; and to detect abuse, apply rate limits and keep the service running.

We do not use your information for advertising, for profiling, or for any purpose you did not ask for.

6. Who We Share Your Information With

6.1 Data brokers and people-search sites

This is the core of what the App does, so it deserves to be stated plainly. When you ask us to remove your data, we have to send some of your personal information to the sites that are holding it. An opt-out request that does not identify you cannot be honored.

Depending on each site's requirements, that may include your name, your address history, your phone number, your email address, and — where a site demands it — identity documentation. We send this only to sites where a match to you was actually found, only for the purpose of getting your record deleted, and only after you have initiated a removal request. We never send it anywhere else.

6.2 Service providers

Google Firebase provides our authentication, database, file storage, serverless functions and push notification infrastructure. It processes your anonymous ID, your scan history, your removal requests and any files you upload. See Google's privacy policy at policies.google.com/privacy.

Have I Been Pwned provides the breach and password data. Email addresses are checked against it through our backend; passwords are checked using the anonymized method described in Section 4. See haveibeenpwned.com/Privacy.

Superwall manages our paywalls and subscription state, and receives your anonymous ID, your subscription status and basic device information. See superwall.com/privacy.

Apple processes all in-app purchases and subscriptions. We never see or receive your payment card details. See apple.com/legal/privacy.

Stripe processes payments where a purchase is completed through our web checkout rather than the App Store. Again, we never see your card details. See stripe.com/privacy.

6.3 Legal disclosure

We may disclose information where we are legally required to by valid legal process, or where disclosure is necessary to protect our rights, our users' safety, or the security of the service. Given the nature of this App, we will resist overbroad requests and will notify affected users where we are legally permitted to do so.

7. Data Security

Your data is transmitted over encrypted connections (TLS) and stored on Google Cloud infrastructure with encryption at rest. Database access rules restrict every record to the anonymous account that created it, so one user cannot read another user's scans or removal requests. Every backend function requires an authenticated session before it will run.

We keep your account anonymous specifically so that a breach of our systems would expose as little about you as possible. That said, no method of transmission or storage is completely secure, and we cannot guarantee absolute security.

8. Data Retention and Deletion

Scan history and removal records are kept with your anonymous account so that you can review them, and are retained until you delete them or until we no longer need them to provide the service.

You can delete an individual scan from your history within the App at any time. Removal requests already submitted to a third-party site cannot be recalled by us once filed, because

the request now sits with that site — although the point of the request is that the site deletes your record.

Deleting the App from your device permanently severs your access to the anonymous account and everything under it.

If you would like your data deleted from our systems, email support@decentsoftwares.in. Because accounts are anonymous, please include enough detail for us to identify the relevant records — for example, the email address or phone number you scanned. We will respond within 30 days.

9. Your Rights

Depending on where you live, you may have the right to access the personal information we hold about you, to correct it, to have it deleted, to receive a copy in portable form, to object to or restrict certain processing, and to be free from discrimination for exercising any of these rights.

If you are in the European Economic Area or the United Kingdom, we process your information on the basis of your consent — which you give by choosing to run a scan or submit a removal request — and on the basis of our legitimate interest in operating and securing the service. You may withdraw consent at any time by ceasing to use the relevant feature and requesting deletion.

If you are a California resident, we confirm that we do not sell or share your personal information as those terms are defined under the CCPA and CPRA.

To exercise any of these rights, contact support@decentsoftwares.in.

10. Children's Privacy

Serus AI is not intended for children under 13, and we do not knowingly collect personal information from them. If you believe a child has provided us with personal information, contact support@decentsoftwares.in and we will delete it.

11. International Users and Data Transfers

The App's servers and service providers are located in the United States, so using it involves transferring your information there, where data protection law may differ from that of your own country.

Please also note that the reverse phone lookup and site sweep features currently cover United States records only. Scans run from elsewhere may return no results, and this reflects the coverage of the underlying sources rather than an error.

12. Third-Party Links

The App links out to external websites — data broker opt-out pages, account-closure guides, and similar resources. We do not control those sites and are not responsible for their privacy practices. Please read their policies before providing them with information.

13. Changes to This Policy

We may update this policy from time to time. When we do, we will revise the "Last updated" date above, and for material changes we will notify you in the App. Continuing to use Serus AI after a change takes effect means you accept the revised policy.

14. Contact Us

For any question about this policy, about your data, or to make a privacy request:

Email: **support@decentsoftwares.in**

We aim to reply within 30 days.