

# Privacy Limited Privacy Policy

Effective Date: July 29, 2022

Welcome to Privacy Limited, and thanks for taking the time to read our Privacy Policy.

Privacy Limited has a very simple view of your data:

- We don't want it
- We don't need it
- It's toxic and dangerous, and belongs only to you
- Please don't give it to us.

With that in mind - below we outline what we collect (*almost nothing*), and what we do with it (*even less*).

The services we offer include Denote for Mac, Denote for iOS (together the Denote Apps), our Cloud Syncing service (the Sync Service), and our Website (the Web).

## Information We Collect

### Registering An Account

You must create a Denote account in order to use our Apps and Sync Service. We randomly create a unique ID to represent you, and that is stored at our server. We also ask for a pseudonym that others can use to identify you when you share document with them. We store that too... but you can leave it blank, use your dogs name, or just "Anonymous".

Other information is either encrypted with your key, which we don't know, or is public. An example of public data is your Public Key, which is used so that other people can share stuff with you securely.

We do not record your IP address or any other identifying data. We don't know who you are or where you come from, and we prefer it that way.

### Creating Books, Writing Notes

All other sensitive data that the Apps create, such as books and notes, will either stay on your device, if you are not a subscriber, or be stored in the cloud and shared across your devices if you are a subscriber. In both cases, all sensitive data is *always* encrypted with your key and cannot be read by anyone (including us). This is referred to as End to End Encryption (E2EE) and is the gold standard for data protection.

There is a small amount of "plumbing" data that we store unencrypted *only* if you subscribe to our sync services - for example there might be a record that indicates user *2s34DYTj30n* owns book *822B52F1-552E-4C64-84A8-E91EBC66806B* and shares it with user *6JjgR45Yc23*. We don't encrypt that information, but it tells us nothing about who you are or the contents of the books and notes, it simply makes the service work.

### Information You Share With Others

If you share any of your notes or books with other users, then they, and only they, will be able to read and make changes to those notes and books.

## Location Information

We are not interested in your location data so we don't collect it. Seriously... don't share it.

## Information Stored on Your Mobile Device

All your sensitive data, such as account information, books, notes, is stored encrypted on your devices at all times. Items are *only* decrypted when the app shows them to you e.g. when you are editing something. Then we re-encrypt those items immediately.

## Information Stored In The Cloud

Our cloud service does store your random ID, your pseudonym, your public key and various salts unencrypted. These are all random and do not need to be protected.

The pseudonym is only used to let others know who is sharing information with them, or who they are sharing information to, and can be whatever you like.

The public key is used to securely share information with others.

The salts are used to initialise encryption when connecting to your other devices. These are random numbers.

If you have subscribed, then we also store all your books and notes, but their contents are encrypted with your key which *never* leaves your device. We can't read them even if we wanted to (which we don't).

## Payment Information

If you decide to subscribe to our service, and we hope you will, then you will need to interact with a payment provider such as the AppStore or Google Play. We are not responsible for their policies and practices.

When you subscribe we get a notification that your random user ID has paid until some date. We know nothing else. We don't get sent your apple ID, credit card, email address or any other personal details.

## Communications

If you contact us for support by email, then your message will include your email address. But we don't know which account is yours (unless you tell us, but don't).

## Cookies and Usage Data

We don't collect any information about you when you visit our website. Not even a cookie. Any information in our Web logs is purged regularly, and cannot be tied to your account.

## Information In Transit

While in transit from your device to our servers, *all* information is *also* protected using TLS which is added on top of the End to End Encryption outlined above. This means:

- a) Even your unprotected information is encrypted in transit
- b) Your data is protected from man-in-the-middle attacks

## How We Use Your Information

By and large... we don't. We do keep your random ID so we know which data belongs to you and some of the aforementioned "plumbing" data, but since almost everything else is encrypted, we can't do anything with it.

We don't personalise the service or analyse your information. We will look at load information to ensure the servers don't catch fire.

## How We Share Your Information

We don't.

Note that if *you* decide to share a book with someone else, then we will send them your random ID, public key and pseudonym (which is probably just "Anonymous" anyway). We also send them a copy of the encryption key that will let them access the book - but that key is encrypted using Public Key Encryption, meaning only they can decrypt it.

Other than that - we don't share anything with anyone - and even if we did it would all be encrypted and useless.

## Deleting Your Data

You can delete your account at any time by selecting "Delete all data and account" in settings. Doing this will remove all encrypted data we store, and delete your account. *There is no undo!* We will keep your random ID and public key around for a while to ensure any in-flight un-sharing messages work. Any books you shared with others will disappear along with all of your data.

Did we mention there is *no undo*?

## International Users

Our lack of information storage and ability to delete your data satisfies GDPR rules (EU), CalOPPA (California), PIPEDA (Canada) and others.

We use AWS in the US for data storage because (at the moment) it has the lowest rates. You need not be concerned about the privacy aspects of data storage in the US because everything is encrypted with your key which never leaves your device.

## Contacting Us

If any of this wasn't clear, feel free to contact us at [support@privacy-tools.tech](mailto:support@privacy-tools.tech).

Privacy Limited