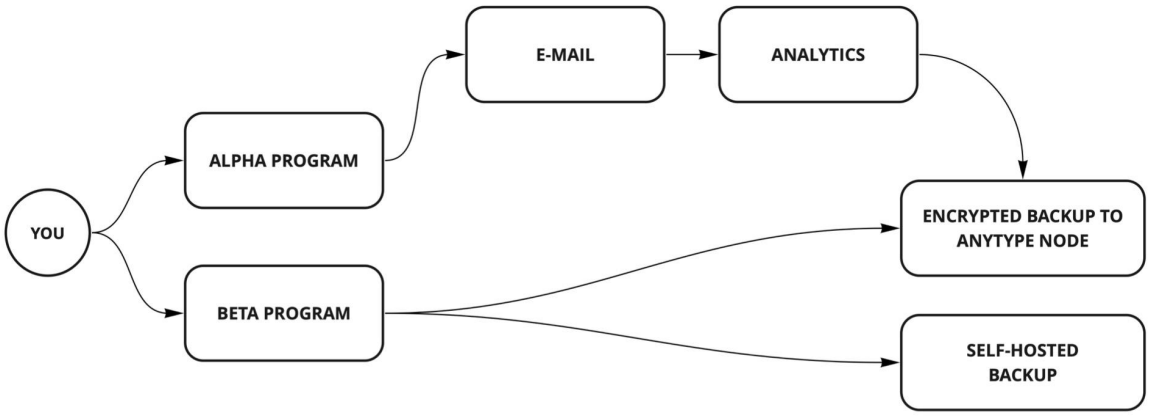
Anytype Privacy Statement

At Anytype, we believe that both individual and collective privacy are fundamental human rights.

In this document, we describe what data we collect in current and future versions of the product, why we collect it, how it is handled, and your rights to it. Our principle is to collect only what we need to make Anytype the best app we can.

Here, we outline the difference between alpha and beta programs with respect to data collection and your choices within each:



The below information is applicable to participants of the alpha program. Once we launch our public beta, you will be able to use Anytype without sharing any information about its usage with us.

Voluntary Correspondence:

Waitlist Signup

When you sign up for our alpha program we ask for your e-mail address.

Upon submission, your e-mail address is stored in our CRM, which we use to assign invite codes, send invitations, and keep track of who has been invited to the app, and on which date.

For alpha testers, an invite code is required to create an account. Upon account creation, your invite code is used to generate an Anytype ID from our server (described in further detail below). Your e-mail address, invite code, and Anytype ID are stored in separate databases.

It is technically possible for the Anytype team to perform custom lookups on our server via an invite code, and link an Anytype ID with the e-mail address to which the code was assigned. However, your Anytype ID is not stored, sent, or shared anywhere with our third-party e-mail service providers.

After inviting you to sign up, we will only use your e-mail to notify you of feature releases and updates on the research & development of Anytype.

Note: For alpha testers who began using the product without submitting an e-mail (for instance if they were referred by a friend), no personally-identifying information is collected.

After launching our public beta, no e-mail address or personally-identifying information will be asked in during any stage of account creation.

Below you will find the links to the privacy policies of our e-mail and CRM service providers. You may opt out of our mailing list by unsubscribing from the e-mails you receive.

- Sendgrid Privacy Policy
- Mailchimp Privacy Policy
- Fibery Privacy Policy

Email Exchange

After signup, when you write to us at Anytype with a question, we keep that correspondence - including your email address - so that we have a history of past correspondence for reference if you contact us in the future.

Typeform Surveys

Surveys you complete on the Anytype website will normally ask for an e-mail address for the purposes of future correspondence. These e-mail addresses are saved in Typeform.

Surveys you complete from the app are anonymized - we do not link them with your Anytype ID or e-mail address.

Involuntary Correspondence:

Web Site Interactions

When you browse our website or any domain of anytype.io, your device automatically shares certain information, such as which operating system and browser you are using. We track the number of website visitors and conversion rates to waitlist signup and download, as well as page load times.

We do not track cookies on our website, nor do we collect any characteristics of protected classifications, including age, race, gender, religion, sexual orientation, gender identity, or gender expression.

You may provide this data voluntarily, for example if you include a pronoun preference in your email signature when writing to our support team.

Here, you can find the privacy policy of our website analytics provider:

- Fathom Analytics Privacy Policy

Product Analytics

Each user is assigned a unique Anytype ID upon creating an account, which consists of a string of numbers and letters that cannot personally identify you. Based on these IDs, we are able to observe product metrics such as session length, number of sessions, and number of Objects, Types, and Templates created.

Our analytics don't reveal any actual content, only the actions you perform in Anytype.

Here, you can find the privacy policy of our app analytics provider:

- Amplitude Analytics Privacy Policy

After our open beta is launched, you will be able to self-host software, in which case the analytics would be disabled by default.

Anytype Backup Node

For alpha testers, any data created within the app is encrypted by the key generated on the user's device before being sent to our backup node ('Cafe node'). This way we don't have any technical ability to read the content stored on our caffe node. Our Cafe node stores:

1) The technical information of each user needed for our sync mechanisms to function properly, including:
    - *ID of user* (public key). We use this to confirm that users' data has not been compromised by other users.
    - *ID of user's devices* (public keys). We use this to confirm that the user's data was not compromised by other devices of the same user.
    - *Date of activation of each account and device.*

- *Hashes and sizes of pinned (stored) encrypted files* you attach to the objects. This allows us to understand how many files each user is storing within Anytype and protects it from malicious use. This also allows us to remove all your files from the backup nodes when requested to do so.
- *IDs of objects in anytype.* This allows us to remove all of your Objects (and the data therein) when you request us to do so.
- *Backed up encrypted objects may contain the last IP address of your devices*. P2P network setup requires us to store the address of nodes for connectivity purposes. We don't use it for any other reason.

2) Encrypted, backed up data from your account. All data created via the Anytype app is stored with encryption in our Cafe node, except for userID and deviceIDs, for resolvability purposes.

   Your data can't be accessed nor collected - only stored. When you need to access it, it is sent back to your device and decrypted locally using your Recovery Phrase. During the alpha program, as we're testing our backup node and seeking to ensure its reliability, sync with our backup node cannot be turned off. Anytype has access to the backup node, but the data is encrypted and we have no private key.

   - *Our Cafe node contains only encrypted backups* and nothing else.
   - Whatever information is created through the app will be stored in Anytype's backup node.

What happens when:

You delete data from your account

In our application, we give you the option to delete data from your Anytype account and bin. Anything you delete will remain accessible to you for 30 days. After that, this data will no longer be accessible through the application and will be deleted from our backup node.

We also have additional backups in case the cafe node is corrupted, which are kept for another 30 days. In total, when data is deleted from your application, it is purged within 90 days from all our systems and records. Data recovery for a single account from a backup is prohibitively expensive, so if you change your mind, you will need to do so before your data is deleted from our backup node.

Law enforcement requires us to share data:

When authorized law enforcement has a necessary warrant, criminal subpoena, or court order requiring us to share data, we make a reasonable effort to inform you, unless we are legally prevented from doing so. It is not possible for Anytype to decrypt your encrypted content, no matter who asks for it, as decryption keys are stored on your device.

Otherwise, we categorically reject requests from local and federal law enforcement authorities when they seek data.

Your Rights with Respect to Your Information

At Anytype, Inc., we apply the same data rights to all customers, regardless of their location. Currently, some of the most important privacy regulations in place are the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") in the United States. Anytype Inc. recognizes all rights granted in these regulations including:

Right to Know: You have the right to know what personal information is collected, used, shared or sold. In this privacy policy, we outline both the categories and specific data we collect, as well as how it is used.

Right of Access: This includes your right to access the personal information we collect about you, and your right to obtain information about the sharing, storage, security, and processing of that information.

Right of Correction: You have the right to request correction of your personal information.

Right to Erase / "Be Forgotten": This is your right to request, subject to certain limitations under applicable law, that your personal information be deleted from our possession and, by extension, from all of our service providers. Fulfilling some data deletion requests may prevent you from using Anytype Inc. services because our requests may then no longer work. In such cases, a data deletion request may result in the closure of your account.

Right to Complaint: You have the right to make a complaint about our handling of your personal information with the appropriate supervisory authority. To identify your specific authority or learn more about this right, EU individuals should go to https://edpb.europa.eu/about-edpb/board/members_en.

Right to Restrict Processing: This is your right to request to restrict how and why your personal information is used or processed, including the option not to sell personal information. (Again: We never have and never will sell your personal information).

Right to object: You have the right, in certain situations, to object to how or why your personal information is processed.

Right to Portability: You have the right to receive the personal information we hold about you and the right to transmit it to another party.

Right not to be subject to automated decision making: You have the right to object and prevent any decision that could have a legal, or similar, effect on you from being made solely on the basis of automated processes. This right is limited, however, if the decision is necessary for the performance of any contract between you and us, is permitted by applicable law, or is based on your explicit consent.

Right to non-discrimination: This right stems from the CCPA. We do and will not charge you a different amount to use our products, offer you different discounts, or give you a lower level of customer service because you have exercised your data privacy rights. However, the exercise of certain rights (such as the right to "be forgotten") may, by virtue of exercising those rights, prevent you from using our Services.

Many of these rights can be exercised by signing in and updating your account information accordingly. If you have questions about exercising these rights or need assistance, please contact us at support@anytype.io.

To identify your specific authority to file a complaint or learn more about GDPR, EU individuals should go to https://edpb.europa.eu/about-edpb/board/members_en.

Privacy Governance

EU-US and Switzerland-US Privacy Protection Policy

The GDPR requires that data transfers outside the EU occur only in countries deemed to have adequate data protection laws. The United States generally does not meet this requirement. The Privacy Shield is an agreement between certain European jurisdictions and the United States that permits the transfer of personal data from the EU to the United States. Participation in the Privacy Shield program is voluntary.

We comply with the frameworks for data from the EU, UK and Switzerland that is transferred to the United States.

Anytype Inc. complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States, respectively. We certify to the Department of Commerce that we adhere to the Privacy Shield Principles. If there is any conflict between the terms of this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles take

precedence. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

Anytype Inc. is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) with respect to the Privacy Shield Framework.

The Privacy Shield Frameworks support specific principles, many of which are already described in the section on your rights. For clarity, under the Privacy Shield Framework, the following principles apply to all data from the EU, UK, and Switzerland that has been transferred to the United States:

You have the right to access your personal data and to update, correct and/or change incomplete information.

You also have the right to request the erasure of personal information that has been processed in violation of the Principles. If you wish to exercise these rights, you may do so by signing in and updating your account information directly. If you have questions about exercising these rights or need assistance, please contact us at support@anytype.io.

Commitment to resolve all complaints

In accordance with the EU-US and Swiss-US Privacy Shield Principles, we are committed to resolving complaints about your privacy and our collection or use of your personal information. Individuals from the European Union, United Kingdom or Switzerland with inquiries or complaints regarding this privacy policy should first contact support@anytype.io.

Anytype Inc. has further committed to refer unresolved privacy complaints under the EU-US and Swiss-US Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by BBB National Programs. If you do not receive a timely acknowledgement of your complaint, or your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/programs/bbb-privacy-shield/eu-dispute-resolution for more information and to file a complaint. This service is provided at no cost to you. Please do not send GDPR complaints to BBB EU Privacy Shield.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may be able to invoke binding arbitration for some residual complaints not resolved by other redress mechanisms. To learn more, please see Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.
Location of the Site and Data

Our products and other web properties are operated in the United States. If you are located in the European Union or elsewhere outside the United States, please be aware that any information you provide to us will be transferred to the United States. By using our site,

participating in any of our services and/or providing us with your information, you consent to this transfer.

Changes and questions

We may update this policy as necessary to comply with relevant regulations and to reflect any new practices. In case of doing so, we will inform you ahead of time and keep previous versions accessible to you.

Do you have any questions, comments, or concerns about this privacy policy, your data, or your rights with respect to your information? Please contact us at support@anytype.io and we will be happy to answer.