

Privacy Notice

1. Introduction
 - 1.1. Compose is a desktop application developed by Quanterium Technologies that allows users to connect multiple messaging accounts into one application
 - 1.2. Quanterium is committed to protect and secure the data of its users following transparent practices
 - 1.3. You can contact us on email on support@compose.im should you have any questions or concerns regarding this document
2. Using the Service means accepting these terms
 - 2.1. By accessing or using the Service in any way, you agree to and are bound by the terms and conditions written in this document
 - 2.2. If you do not agree to all the terms and conditions contained in this document then please do not use this Service
3. This is a living document
 - 3.1. This is a living document and we will likely update this document over time. By continuing to use the Service, you will implicitly accept the changes we make
 - 3.2. Your access and use of the Service is always subject to the most current version of this document
4. Definitions
 - 4.1. Compose is a desktop application referred as “Application” or “Service”, owned by Quanterium Technologies (referred to as “I”, “Me”, “We” or “Quanterium”)
 - 4.2. Anyone using this Application will be referred to as “User” or “You”
 - 4.3. External services like WhatsApp, Slack, Gmail... will be referred to as “Third-Party Services”
5. Data erasure
 - 5.1. All user data is held locally on the user’s machine and sent directly to Third-Party Services as per those services’ requirements. Please refer to the relevant Third-party service’s privacy policy for more information.
6. Data portability
 - 6.1. Under GDPR you have a right to request a copy of your data in a commonly-accepted format
 - 6.2. If you would like a copy of your data, please send a request to support@compose.im
7. Your rights as a data subject
 - 7.1. You have rights in relation to the personal data we hold about you. Some of these only apply in certain circumstances. Some of these rights are explored in more detail elsewhere in this document. For completeness, your rights under GDPR are:
 - 7.1.1. The right to be informed
 - 7.1.2. The right of access
 - 7.1.3. The right to rectification
 - 7.1.4. The right to erasure

- 7.1.5. The right to restrict processing
 - 7.1.6. The right to data portability
 - 7.1.7. The right to object
 - 7.1.8. Rights in relation to automated decision making and profiling
- 7.2. For more details about these rights, please see [the guidance provided by the ICO](#)
- 8. What information we collect and why?
 - 8.1. We collect information about you when you input it into the Service or otherwise provide it directly to us
 - 8.2. Account and Profile Information:
 - 8.2.1.1. Your email address
 - 8.2.1.2. Password
 - 8.2.1.3. Username
 - 8.2.2. Your username and password is used to authenticate your access to the Service and to uniquely identify you within the Service
 - 8.2.3. We will use your email address to let you reset your password if you forget it, and to send you notifications about missed messages from users trying to contact you if you enable the option. We may also send you infrequent updates
 - 8.3. Device and connection information
 - 8.3.1. Each device you use to access the Service is allocated an identifier. When you access the Service, we record the device identifier, the IP address is used to connect, user agent, and the time at which it last connected to the service
 - 8.3.2. This information is gathered to help you to manage your devices - you can view and manage the list of devices by connecting to the Service
 - 8.3.3. IP addresses are also used to mitigate abuse, debug operational issues, and monitor traffic patterns. Our logs are kept for no longer than 180 days
- 9. Additional Limits on Use of Your Google User Data: Notwithstanding anything else in this Privacy Policy, if you provide the App access to the following types of your Google data, the App's use of that data will be subject to these additional restrictions:
 - 9.1. The App will only use access to read, write, modify, or control Gmail message bodies (including attachments), metadata, headers, and settings to provide a web email client that allows users to compose, send, read, and process emails and will not transfer this Gmail data to others unless doing so is necessary to provide and improve these features, comply with applicable law, or as part of a merger, acquisition, or sale of assets.
 - 9.2. The App will not use this Gmail data for serving advertisements.
 - 9.3. The App will not allow humans to read this data unless we have your affirmative agreement for specific messages, doing so is necessary for security purposes such as investigating abuse, to comply with applicable law, or for the App's internal operations and even then only when the data have been aggregated and anonymized.
- 10. What information is shared with third parties and why?

- 10.1. Sharing data with connected services
 - 10.1.1. Third-Party Integrations
 - 10.1.1.1. Some Compose chats are integrations to third-party services, such as WhatsApp, Telegram or Gmail.
 - 10.1.1.2. By integrating with third-party services you accept their respective privacy policies. We have no control over how these services handle your data and it is with you to decide which ones you trust
 - 10.1.1.3. Bridged services can be located anywhere in the world, and are subject to local laws and regulations
 - 10.1.1.4. We do not store your password nor do we directly access your messaging service's account for any third-party services
 - 10.1.1.5. If this is not acceptable to you, please do not use the integration.
11. Sharing data
 - 11.1. In exceptional circumstances, we may share information about you with a third party if we believe that sharing is reasonably necessary to
 - 11.1.1. Comply with any applicable law, regulation, legal process or government request
 - 11.1.2. Protect the security or integrity of our products and services (e.g. for a security audit)
 - 11.1.3. Protect Quanterium Technologies and our users from harm or illegal activities
 - 11.1.4. Respond to an emergency which we believe in good faith requires us to disclose information to assist in preventing the serious bodily harm of any person
12. Who can see my messages and files?
 - 12.1. Compose has no visibility on any of your messages or files across any third-party service.
 - 12.2. In third-party providers, messages and content are never transmitted to Quanterium Technologies servers, unless explicitly mentioned.
13. Who else has access to my data?
 - 13.1. We host the Service in Amazon Web Services (AWS) data centres and store some files shared there as well
 - 13.2. AWS employees have access to this data. Here's [Amazon's privacy policy](#). Amazon controls physical access to their locations
 - 13.3. Physical access to our offices and locations use typical physical access restrictions
 - 13.4. We use secure private keys when accessing servers via SSH, and protect our AWS console passwords locally with a password management tool
14. How do you handle passwords?
 - 14.1. We never store password data in plain text; instead, they are stored hashed (with at least 12 rounds of bcrypt, including both a salt and a server-side pepper secret). Passwords sent to the server are encrypted using SSL

- 14.2. It is your sole responsibility to keep your username, password and other sensitive information confidential. Actions taken using your credentials shall be deemed to be actions taken by you, with all consequences including service termination, civil and criminal penalties
- 14.3. If you become aware of any unauthorized use of your account or any other breach of security, you must notify Quanterium Technologies immediately by sending an email to support@compose.im.
- 14.4. If you forget your password (and you have registered an email address) you can use the password reset facility to reset it.
- 14.5. We will never change a password for you
15. How can I access or correct my information?
 - 15.1. You can access all your personally identifiable information in the Settings section. You can download a copy of all your data as per the “Data portability” section by sending a request for “Data portability” to support@compose.im
16. Children’s privacy
 - 16.1. We never knowingly collect or maintain information in the Service from those we know are under 16, and no part of the Service is structured to attract anyone under 16.
 - 16.2. If you are under 16, please do not use the Service
17. What should I do if I find a security vulnerability in the Service?
 - 17.1. If you have discovered a security concern, please email us at support@compose.im
 - 17.2. We’ll work with you to make sure that we understand the scope of the issue, and that we fully address your concern
 - 17.3. We consider correspondence sent to support@compose.im our highest priority and work to address any issues that arise as quickly as possible
 - 17.4. Please act in good faith towards our users’ privacy and data during your disclosure. White hat security researchers are always appreciated
18. Making a complaint
 - 18.1. We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention at support@compose.im if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.
 - 18.2. If you want to make a complaint about the way we have processed your personal information to the supervisory authority, you can contact the ICO (the statutory body which oversees data protection law) at <https://www.ico.org.uk/concerns>.