Privacy Policy

Welcome to Filterly

Filterly operates the website and SaaS platform accessible via [filterly.ai] (hereinafter referred to as the “Service”).

This Privacy Policy governs your use of the Service and explains how we collect, use, safeguard, and disclose information that results from your use of our platform, including data from connected Gmail accounts, X (Twitter) messages, and user preferences.

By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used herein have the same meanings as in our Terms and Conditions.

Our Terms and Conditions (“Terms”) govern all use of our Service and, together with this Privacy Policy, constitute the full agreement between you and us (“agreement”).

Definitions

- **Service** means the SaaS product and website accessible via [filterly.ai], operated by Filterly.

- **Personal Data** means data about a living individual who can be identified from that data (or from those and other information either in our possession or likely to come into our possession).

- **Usage Data** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, diagnostic logs, time spent on certain pages, or feature usage).

- **Cookies** are small files stored on your device (computer or mobile device) that may be used to improve functionality, remember user settings, or for analytics.

- **Data Controller** means a natural or legal person who (alone, or jointly with others) determines the purposes and means of processing personal data. For purposes of this Privacy Policy, Filterly is the Data Controller of your personal data.

- **Data Processor (or Service Provider)** means any natural or legal person who processes the data on behalf of the Data Controller. We may use the services of third-party providers (e.g., OpenAI, cloud storage vendors) to process your data effectively and securely.

- **Data Subject** refers to any living individual who is the subject of Personal Data.

- **User** refers to the individual using our Service. The User corresponds to the Data Subject, whose personal data is processed as part of the Service.

Information Collection and Use

We collect several types of information to provide and improve the Service. This includes information you actively provide (like OAuth authorization), messages and emails you explicitly connect for analysis, and data collected automatically (such as usage metrics). More details are provided in the following sections.

1. Introduction

We at Filterly are committed to protecting your privacy. This Privacy Policy describes the information we collect from users of our service (the “Service”), which processes your emails, direct messages on X (formerly Twitter), and your personal preferences. It also explains how we use and share that information, your rights regarding your data, and how we safeguard your information. By using Filterly, you agree to the collection and use of information in accordance with this Privacy Policy. We comply with the EU General Data Protection Regulation (GDPR) and other applicable privacy laws in the jurisdictions where we operate.

2. Information We Collect

We collect several types of information to provide and improve our Service, including:

- **Account Information:** When you register for Filterly, we collect information you provide during sign-up. This may include your name, email address, password (which is stored in hashed form), and/or information from third-party OAuth providers. If you register or log in via Google or X (Twitter), we receive basic profile details such as your username, email, and profile picture from those services.

- **Connected Account Data (Emails and Messages):** If you choose to connect your email account or X (Twitter) account to Filterly, we will access and process the content of your emails and direct messages. Filterly only retrieves the data necessary to perform the requested analysis on your communications. This may include email subject lines, bodies, attachments, and metadata, as well as the text of direct messages on X. We access this information **only with your explicit authorization** and in accordance with the permissions you grant.

- **User Preferences and Settings:** We collect any personal preferences, settings, or customization you provide within the Service. For example, this can include categories or filters you set, language preferences, notification settings, or other configuration data that personalizes your experience.

- **Usage Data:** We automatically collect certain information about how you use Filterly. This includes log data such as the dates and times you access the Service, features you use, credits consumed, and interactions with our user interface. We may also collect device and browser information (e.g. IP address, browser type, device type, operating system) and cookies or similar tracking technologies to remember your session, preferences, and for security (for example, to keep you logged in).

- **Payment Information:** If you purchase additional credits or any paid features, our third-party payment processor (e.g. credit card provider or payment platform) will collect and process your payment information. Filterly itself does **not** store full credit card numbers or banking details; however, we may keep records of your purchases, transaction dates, and amounts for billing and accounting purposes.

3. How We Use Your Information

Filterly uses the collected information for the following purposes:

- **Providing and Improving the Service:** We use your information to operate Filterly and provide you with the Service's core functionality – for example, accessing your authorized emails and X messages, processing them with our AI to generate analysis or scores, and delivering those results back to you. We also use data to maintain and improve the Service's performance, develop new features, and refine our algorithms and user experience.

- **AI Processing of Content:** Part of our Service involves analyzing the text of your emails and messages using artificial intelligence. To accomplish this, your message content may be sent to our AI processing provider (for example, the OpenAI API) for analysis and scoring. This processing is automated and is solely used to generate the results (such as an AI-generated score or summary) that we then provide to you. Our third-party AI provider is **contractually prohibited** from using your data for any purpose other than providing this analysis; for instance, data submitted through the OpenAI API is not used to train OpenAI's models or improve their services by default.

- **Communication:** We use contact information (like your email) to send you service-related communications and notifications. These include confirmations of account creation, information on credit usage or expiration, alerts about analysis results, important security or support messages, and updates about our Service. If you agree or as permitted by law, we may also send occasional marketing communications about new features or promotions; you will have the option to opt out of such marketing emails.

- **Payments and Credits Management:** We use your information to track your credit balance and purchases. For example, we'll inform you when your included credits are running low, and process transactions when you buy additional credits. Transactional emails or receipts may be sent for your records.

- **Customer Support:** If you contact us for help, bug reporting, or feedback, we will use your contact information and any provided details to respond to you and resolve issues. We may also use your feedback to improve the Service.

- **Legal Compliance and Security:** We may process your personal information as required to comply with applicable laws, regulations, and legal obligations (such as tax and accounting requirements or responding to lawful requests by authorities). Additionally, we use information to enforce our Terms and Conditions, to detect, prevent and address fraud, abuse, and security issues. This includes using usage data and automated tools to monitor for suspicious or unauthorized activities on the Service.

4. Legal Basis for Processing (GDPR)

If you are located in the European Economic Area (EEA) or United Kingdom, we rely on certain legal bases under the GDPR to process your personal data:

- **Performance of a Contract:** Most data we collect (emails, messages, account info) is processed on the basis that it is necessary for us to provide the Service that you have requested under our Terms and Conditions. For example, we cannot analyze your messages and provide results without accessing and processing the content you authorize us to use.

- **Consent:** We rely on your consent in situations where you connect third-party accounts (granting us permission to access your data), or where you have opted in to receive marketing communications. You have the right to withdraw consent at any time, though note that this will not affect processing already performed.

- **Legitimate Interests:** In some cases, we process data for purposes of our legitimate interests, balanced against your data protection rights. For instance, maintaining the security of our Service, improving and developing new features, and providing customer support are in our legitimate interests. When we rely on legitimate interest, we ensure that our interests are not overridden by your privacy rights.

- **Legal Obligation:** We will process personal data if necessary to comply with a legal obligation, such as retaining certain transaction records for financial regulations or responding to court orders.

5. How We Share Your Information

We value your privacy and **we do not sell your personal information** to third parties. However, we do share certain information in the following circumstances to run our Service:

- **Service Providers:** We use trusted third-party service providers to help us operate and improve Filterly. These include:

    - *Cloud Storage and Hosting:* We may store your information on cloud infrastructure (servers/databases) provided by reputable companies (for example, AWS, Google Cloud, or others). These providers may process and store data on our behalf, but only under strict security standards and contractual obligations that protect your data.

    - *AI Processing Partner:* As noted, we send message content (which may include personal data) to our artificial intelligence partner, such as OpenAI,

to analyze and score the content. This third party acts as a data processor on our behalf. They are bound by confidentiality and data protection agreements. According to OpenAI's policies, data submitted via their API is not used to train their models or for any purpose other than providing the requested analysis. As part of our service, Filterly may process message content through trusted third-party AI providers (e.g., OpenAI, Google Gemini) for analysis and scoring. These providers are contractually bound not to use the data for training or other purposes.

    - *Authentication Providers:* If you sign up or log in through Google or X (Twitter), those services will authenticate your identity. In doing so, you are sharing certain information (such as your login credentials or tokens) with them and with us (such as your Google or X profile information). Google's and X's use of your data provided for login is governed by their own privacy policies. We receive and use the data from them as described in "Account Information" above.

    - *Payment Processors:* When you purchase credits or paid subscriptions, payments are handled by third-party processors (e.g. Stripe, PayPal, or similar). These processors will handle your credit card or payment account details securely. We share with them only the information necessary to execute the transaction (such as your user ID or email and the purchase amount). Payment processors may have their own legal or regulatory obligations to retain your information. We do not store your sensitive payment details on our systems.

    - *Other Contractors:* We may also engage other vendors for functions such as email delivery (for sending verification emails, notifications), analytics (to understand how users use our Service and improve it), or customer support tools. These parties only get limited information as needed for their role and are obligated to protect it.

- **Legal Requirements and Protection:** We may disclose your information if required to do so by law or in response to valid requests by public authorities (e.g., law enforcement or government agencies). We may also share information when we believe in good faith that disclosure is necessary to protect our rights, your safety or the safety of others, investigate fraud or security issues, or respond to a government request.

- **Business Transfers:** If Filterly is involved in a merger, acquisition, investment, financing, reorganization, or sale of all or a portion of our business, your information may be transferred to the parties involved in the transaction as part of due diligence or the final transfer. In such cases, we will ensure that the new owner will continue to be bound by terms that protect your personal data, and we will notify you of any change in data ownership or use.

- **With Your Consent:** We will share your personal information with other parties outside of the above circumstances only with your consent or at your direction. For example, if in the future we offer an integration with another service and you explicitly opt-in to share data with that service, we will do so only with your permission.

6. Data Storage and Security

We understand the importance of securing your personal data. Filterly implements appropriate technical and organizational measures to protect your information against unauthorized access, alteration, disclosure, or destruction. Key security practices include:

- **Encryption:** All data is transmitted over secure channels using SSL/TLS encryption. The emails, messages, and personal data we store in our database are encrypted at rest. This means that your data is stored in an encrypted format in our databases or storage systems, adding an extra layer of protection in case of unauthorized access to storage.

- **Access Controls:** Only authorized personnel and contractors with a need to know your information to perform their duties have access to the systems that store personal data. Strict access controls, authentication measures, and employee training are in place to prevent unauthorized internal access.

- **Security Testing:** We regularly update and patch our software and infrastructure to address security vulnerabilities. Periodic security audits, code reviews, and penetration testing may be conducted to ensure our systems remain secure.

- **Limited Data Access:** As a policy, we do not proactively read your message content. The processing of your emails and DMs is automated. Human access to your raw content is limited to exceptional cases (for example, if you request support that requires looking into data, or for debugging a specific issue, and only

with your consent or to the extent permitted by law).

- **Third-Party Security:** We carefully select our third-party service providers and require them to have security practices that meet high standards. For example, our cloud and AI providers maintain industry-standard security certifications (such as SOC 2, ISO 27001) and comply with privacy regulations like GDPR. We also enter into Data Processing Agreements (DPAs) with relevant providers to ensure they protect personal data in line with this Privacy Policy and applicable law.

Despite our efforts, no security measure is 100% infallible. We therefore cannot guarantee absolute security of data. However, we strive to protect your personal information and regularly review our security procedures to adapt to new threats. In the unlikely event of a data breach that affects your personal data, we will notify you and the appropriate authorities as required by law.

7. Data Retention

We retain personal information only for as long as necessary to fulfill the purposes outlined in this Privacy Policy or as required by law:

- **Account Information:** We keep your account profile information for as long as your account is active. If you delete your account or request deletion, we will remove or anonymize your personal data within a reasonable time, except for information we are required to retain by law (for example, records of transactions for financial reporting, or logs needed for security and fraud prevention).

- **Emails and Messages Content:** The content of emails and X DMs that you have imported or that we have processed may be stored on our servers to enable features like re-analysis, history, or audit trails for your reference. However, we do not retain this content longer than necessary. Users can delete their data or disconnect accounts at any time to remove stored message content. By default, if you delete a particular email or message from the Service (or disconnect an integrated account), we will delete the associated content from our active databases. In any case, message content and analysis results are typically retained no longer than needed to provide the analysis and related features, unless you request otherwise.

- **AI Processing Data:** Any data sent to our AI processing provider (OpenAI or similar) is not stored by them long-term for their own purposes. According to their

policies, API request data may be retained temporarily (e.g., up to 30 days by OpenAI) solely for monitoring abuse and debugging, after which it is deleted.

- **Usage Logs:** We may retain logs of access and usage (which may include IP addresses, timestamps, and activity records) for a limited period for security, auditing, and analytics. Typically, basic logs are kept for a few months up to a year, unless longer retention is necessary (for example, investigating abuse or fulfilling legal obligations).

- **Backups:** Our systems may maintain backup copies of data for disaster recovery. These backups are encrypted and stored securely. Even after data is deleted from our active database, it might remain in encrypted backups for a short duration until those backups are rotated and overwritten. We ensure that any retained backups are protected and eventually deleted or anonymized according to our data retention policies.

- **Legal Requirements:** In certain cases, we may need to retain information for longer periods if required by law. For instance, financial records of purchases may be kept for the legally required period (e.g., for tax or accounting regulations). Similarly, we may retain certain data as necessary to resolve disputes or enforce our agreements.

Once the retention period expires or the purpose for processing is fulfilled, we will securely delete or anonymize your information so that it can no longer be attributed to you.

8. Your Rights and Choices

You have rights regarding your personal information, and we are committed to providing you control over your data. Depending on your location and the applicable laws (such as GDPR if you are in the EEA or UK), your rights may include:

- **Access and Portability:** You have the right to request a copy of the personal data we hold about you, and to receive it in a structured, commonly used, machine-readable format. This allows you to transmit your data to another service if needed.

- **Correction:** You may correct or update your personal information if it is inaccurate or incomplete. Much of your account information can be updated through your profile settings. For any data that you cannot update yourself, you

can contact us to request correction.

- **Deletion (Right to be Forgotten):** You have the right to request the deletion of your personal data. For example, you can delete your account or specific content via the Service interface. You may also contact us to request full removal of your data. We will honor such requests to the extent required by law, though please note we may retain certain information as described in our **Data Retention** section (e.g., for legal obligations). You may request deletion of your data at any time via your account settings or by contacting support.

- **Restriction of Processing:** You can ask us to restrict the processing of your data in certain circumstances – for instance, if you contest the accuracy of the data or if the processing is unlawful but you prefer restriction over deletion. This means we would store your data but not actively use it until the issue is resolved (aside from maintaining the restriction).

- **Objection to Processing:** You have the right to object to certain types of processing, such as processing for direct marketing or when we process data based on legitimate interests. In such cases, we will stop processing the data unless we have compelling legitimate grounds to continue or as permitted by law. For marketing emails, you can always opt out by using the “unsubscribe” link in the message or adjusting your account email preferences.

- **Withdraw Consent:** If we rely on your consent for any processing (e.g., if you explicitly consented to optional data collection or to receive marketing), you have the right to withdraw that consent at any time. Withdrawing consent will not affect the lawfulness of any processing we conducted prior to your withdrawal.

- **Non-Discrimination:** If you exercise any of your rights, we will not discriminate against you. For example, if you choose to exercise privacy rights, we will not deny you service or provide you a different level of service, except as permitted by law (note that deletion of certain data may affect our ability to provide the Service features).

- **Complaints:** If you believe that our handling of your personal data violates your rights or applicable privacy laws, you have the right to lodge a complaint with a supervisory data protection authority. If you are in the EEA, you can contact the data protection authority in your country. If you are in the UK, you can contact the Information Commissioner’s Office (ICO). We would, however, appreciate the chance to address your concerns first – please feel free to contact us directly so

we can discuss any issue.

Exercising Your Rights: You can exercise many of the above rights by logging into your Filterly account and using the settings or tools provided (for example, to download data or delete content). Alternatively, you may contact us at the email address provided in the Contact section below to make any requests. For security, we may need to verify your identity before fulfilling certain requests (such as accessing or deleting substantial data), to ensure that these rights are exercised by the correct individual. We will respond to your request within a reasonable timeframe and in accordance with applicable law (typically within 30 days).

9. International Data Transfers

Filterly is a global service. By using the Service, you acknowledge that your personal data may be transferred to and processed in countries other than your own. These countries may have data protection laws different from (and potentially less stringent than) the laws in your jurisdiction. Specifically, our servers, support team, or service providers (such as cloud hosting or OpenAI's processing servers) may be located in **the United States and other countries**.

However, whenever we transfer personal data out of regions like the European Union/EEA, we take steps to ensure an adequate level of protection for your data in accordance with GDPR and other regulations. These safeguards may include:

- **Standard Contractual Clauses:** We may use EU Commission-approved Standard Contractual Clauses (SCCs) in our contracts with service providers or affiliates to ensure that they protect EEA/UK personal data according to EU standards when it is processed outside the EEA.

- **Adequacy Decisions:** In cases where your data is transferred to a country that the EU deems to have adequate data protection laws (an "adequacy decision"), we rely on that decision for the transfer.

- **Privacy Frameworks:** Where applicable, we may adhere to recognized data protection frameworks, such as the EU-US Data Privacy Framework or similar, once effective and if they apply to our service providers.

- **Other Safeguards:** We ensure that all third parties handling personal data have committed to robust privacy practices. This includes encryption in transit and at rest, and compliance with standards like GDPR. We also enter into Data

Processing Agreements as needed, which contractually bind our processors to protect your data.

If you would like more information about the international transfer of your data or the safeguards in place, please contact us. By using Filterly, you consent to your information being transferred to our facilities and to the facilities of those third parties with whom we share it, as described in this policy.

10. Children's Privacy

Filterly is not directed to children, and we do not knowingly collect personal information from individuals under the age of 13 (or the minimum age required by local law, such as 16 under GDPR in certain EU member states). If you are not old enough to legally use our Service, please do not provide us with your personal information, including your name, email, or any message content.

Parents or legal guardians should supervise their children's internet usage and are responsible for ensuring that children do not access services that are not age-appropriate. If we become aware that we have inadvertently collected personal data from a child without appropriate consent, we will take steps to delete that information promptly. If you believe that a child under the relevant age may have provided us personal information, please contact us immediately so that we can investigate and remove the data as necessary.

11. Changes to this Privacy Policy

We may update or revise this Privacy Policy from time to time as our services and legal requirements evolve. Filterly reserves the right to change our Privacy Policy, but we will provide prior notice of any significant changes. We will notify you of material changes by email (sent to the address associated with your account) or by prominently posting a notice on our website or within the app **before** the change becomes effective. The "Last Updated" date at the top of this Policy will reflect the date of the latest revisions.

We encourage you to review this Privacy Policy periodically for any updates. Continued use of the Service after any changes to the Privacy Policy have become effective indicates your acceptance of the revised terms. If you do not agree with the changes, you should stop using the Service and may request deletion of your data.

12. Contact Us

Filterly adheres to Google's Limited Use requirements for Gmail data.

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

Filterly **– Privacy Team**
Email: nico@filterly.ai

We will gladly address your inquiries and work with you to resolve any concerns about your privacy. Your trust is important to us, and we are committed to safeguarding your personal information.