Terms of Service

Thank you for using our products! We build them to help you do your best work.

When we say “Company”, “we”, “our”, or “us” in this document, we are referring to Outreachbot.

When we say “Services”, we mean our website outreachbot.com. That includes all our product and content whether delivered within a web browser, desktop application, mobile application, or another format.

When we say “You” or “your”, we are referring to the people or organizations that own an account with our Service.

We may update these Terms of Service ("Terms") in the future. Typically these changes have been to clarify some of these terms by linking to an expanded related policy. Whenever we make a significant change to our policies, we will refresh the date at the top of this page and take any other appropriate steps to notify account holders.

When you use our Services, now or in the future, you are agreeing to the latest Terms. There may be times where we do not exercise or enforce a right or provision of the Terms; however, that does not mean we are waiving that right or provision. **These Terms do contain a limitation of our liability.**

If you violate any of the Terms, we may terminate your account. That’s a broad statement and it means you need to place a lot of trust in us. We do our best to deserve that trust by being open about keeping an open door to your feedback: info@outreachbot.com.

Account Terms

1. You are responsible for maintaining the security of your account and password and for ensuring that any of your users do the same. The Company cannot and will not be liable for any loss or damage from your failure to comply with this security obligation.
2. You may not use the Services for any purpose outlined in our Use Restrictions policy, and you may not permit any of your users to do so, either.
3. You are responsible for all content posted to and activity that occurs under your account, including content posted by and activity of any users in your account.
4. You must be a human. Accounts registered by “bots” or other automated methods are not permitted.

Payment, Refunds, and Plan Changes

1. If you are using a free version of one of our Services, it is really free: we do not ask you for your credit card and — just like for customers who pay for our Services — we do not sell your data.

2. For paid Services that offer a free trial, we explain the length of trial when you sign up. After the trial period, you need to pay in advance to keep using the Service. If you do not pay, we will freeze your account and it will be inaccessible until you make payment. If your account has been frozen for a while, we will queue it up for auto-cancellation. See our Cancellation policy for more details.
3. If you are upgrading from a free plan to a paid plan, we will charge your card immediately and your billing cycle starts on the day of upgrade. For other upgrades or downgrades in plan level, the new rate starts from the next billing cycle.
4. All fees are exclusive of all taxes, levies, or duties imposed by taxing authorities. Where required, we will collect those taxes on behalf of the taxing authority and remit those taxes to taxing authorities. Otherwise, you are responsible for payment of all taxes, levies, or duties.
5. We process refunds according to our Fair Refund policy.

Cancellation and Termination

1. You are solely responsible for properly canceling your account. You can find instructions for how to cancel your account in our Cancellation policy. An email or phone request to cancel your account is not automatically considered cancellation. If you need help canceling your account, you can always contact our support team info@outreachbot.com.
2. All of your content will be inaccessible from the Services immediately upon account cancellation. Within 30 days, all content will be permanently deleted from active systems and logs. Within 60 days, all content will be permanently deleted from our backups. We cannot recover this information once it has been permanently deleted.
3. If you cancel the Service before the end of your current paid up month, your cancellation will take effect immediately, and you will not be charged again. We do not automatically prorate unused time in the last billing cycle. See our Fair Refund policy for more details.
4. We have the right to suspend or terminate your account and refuse any and all current or future use of our Services for any reason at any time. Suspension means you and any other users on your account will not be able to access the account or any content in the account. Termination will furthermore result in the deletion of your account or your access to your account, and the forfeiture and relinquishment of all content in your account. We also reserve the right to refuse the use of the Services to anyone for any reason at any time. We have this clause because statistically speaking, out of the hundreds of thousands of accounts on our Services, there is at least one doing something nefarious. There are some things we staunchly stand against and this clause is how we exercise that stance. For more details, see our Use Restrictions policy.
5. Verbal, physical, written or other abuse (including threats of abuse or retribution) of a Company employee or officer will result in immediate account termination.

Modifications to the Service and Prices

1. We make a promise to our customers to support our Services. That means when it comes to security, privacy, and customer support, we will continue to maintain any legacy Services. Sometimes it becomes technically impossible to continue a feature or we redesign a part of our Services because we think it could be better or we decide to close new signups of a product. We reserve the right at any time to modify or discontinue, temporarily or permanently, any part of our Services with or without notice.
2. Sometimes we change the pricing structure for our products. When we do that, we tend to exempt existing customers from those changes. However, we may choose to change the prices for existing customers. If we do so, we will give at least 30 days notice and will notify you via the email address on record. We may also post a notice about changes on our websites or the affected Services themselves.

Uptime, Security, and Privacy

1. Your use of the Services is at your sole risk. We provide these Services on an "as is" and "as available" basis. We do not offer service-level agreements for most of our Services but do take uptime of our applications seriously.
2. We reserve the right to temporarily disable your account if your usage significantly exceeds the average usage of other customers of the Services. Of course, we'll reach out to the account owner before taking any action except in rare cases where the level of use may negatively impact the performance of the Service for other customers.
3. We take many measures to protect and secure your data through backups, redundancies, and encryption. We enforce encryption for data transmission from the public Internet. There are some edge cases where we may send your data through our network unencrypted. Please refer to our Security Overview for full details and our Security Response page for how to report a security incident or threat.
4. When you use our Services, you entrust us with your data. We take that trust to heart. You agree that Outreachbot may process your data as described in our Privacy Policy and for no other purpose. We as humans can access your data for the following reasons:

- **To help you with support requests you make.** We'll ask for express consent before accessing your account.
- **On the rare occasions when an error occurs that stops an automated process partway through.** We get automated alerts when such errors occur. When we can fix the issue and restart automated processing without looking at any personal data, we do. In rare cases, we have to look at a minimum amount of personal data to fix the issue. In these rare cases, we aim to fix the root cause to prevent the errors from recurring.
- **To safeguard Outreachbot.** We'll look at logs and metadata as part of our work to ensure the security of your data and the Services as a whole. If necessary, we may also access accounts as part of an abuse report investigation.
- **To the extent required by applicable law.** As a US company with all data infrastructure located in the US, we only preserve or share customer data if

compelled by a US government authority with a legally binding order or proper request under the Stored Communications Act, or in limited circumstances in the event of an emergency request. If a non-US authority approaches Outreachbot for assistance, our default stance is to refuse unless the order has been approved by the US government, which compels us to comply through procedures outlined in an established mutual legal assistance treaty or agreement mechanism. If Outreachbot is audited by a tax authority, we only share the bare minimum billing information needed to complete the audit.

5. We use third party vendors and hosting partners to provide the necessary hardware, software, networking, storage, and related technology required to run the Services.
6. Under the California Consumer Privacy Act ("CCPA"), Outreachbot is a "service provider", not a "business" or "third party", with respect to your use of the Services. That means we process any data you share with us only for the purpose you signed up for and as described in these Terms, the Privacy policy, and other policies. We do not retain, use, disclose, or sell any of that information for any other commercial purposes unless we have your explicit permission. And on the flip-side, you agree to comply with your requirements under the CCPA and not use Outreachbot's Services in a way that violates the regulations.
7. These Terms incorporate the Data Processing Addendum ("DPA") when the EU General Data Protection Regulation ("GDPR") or United Kingdom General Data Protection Regulation ("UK GDPR") applies to your use of Outreachbot Services to process Customer Data as defined in the DPA. The DPA linked above supersedes any previously agreed data processing addendum between you and Outreachbot relating to your use of the Outreachbot Services.

Copyright and Content Ownership

1. All content posted on the Services must comply with U.S. copyright law.
2. You give us a limited license to use the content posted by you and your users in order to provide the Services to you, but we claim no ownership rights over those materials. All materials you submit to the Services remain yours.
3. We do not pre-screen content, but we reserve the right (but not the obligation) in our sole discretion to refuse or remove any content that is available via the Service.
4. The Company or its licensors own all right, title, and interest in and to the Services, including all intellectual property rights therein, and you obtain no ownership rights in the Services as a result of your use. You may not duplicate, copy, or reuse any portion of the HTML, CSS, JavaScript, or visual design elements without express written permission from the Company. You must request permission to use the Company's logos or any Service logos for promotional purposes. Please email us at info@outreachbot.com equests to use logos. We reserve the right to rescind any permissions if you violate these Terms.
5. You agree not to reproduce, duplicate, copy, sell, resell or exploit any portion of the Services, use of the Services, or access to the Services without the express written permission of the Company.

Features and Bugs

We design our Services with care, based on our own experience and the experiences of customers who share their time and feedback. However, there is no such thing as a service that pleases everybody. We make no guarantees that our Services will meet your specific requirements or expectations.

We also test all of our features extensively before shipping them. As with any software, our Services inevitably have some bugs. We track the bugs reported to us and work through priority ones, especially any related to security or privacy. Not all reported bugs will get fixed and we don't guarantee completely error-free Services.

Services Adaptations and API Terms

We offer Application Program Interfaces ("API"s) for some of our Services. Any use of the API, including through a third-party product that accesses the Services, is bound by these Terms plus the following specific terms:

1. You expressly understand and agree that we are not liable for any damages or losses resulting from your use of the API or third-party products that access data via the API.
2. Third parties may not access and employ the API if the functionality is part of an application that remotely records, monitors, or reports a Service user's activity *other than time tracking*, both inside and outside the applications. The Company, in its sole discretion, will determine if an integration service violates this bylaw. A third party that has built and deployed an integration for the purpose of remote user surveillance will be required to remove that integration.
3. Abuse or excessively frequent requests to the Services via the API may result in the temporary or permanent suspension of your account's access to the API. The Company, in its sole discretion, will determine abuse or excessive usage of the API. If we need to suspend your account's access, we will attempt to warn the account owner first. If your API usage could or has caused downtime, we may cut off access without prior notice.

Some third-party providers have created integrations between our Services and theirs. We are not liable or accountable for any of these third-party integrations.

Liability

We mention liability throughout these Terms but to put it all in one section:

You expressly understand and agree that the Company shall not be liable, in law or in equity, to you or to any third party for any direct, indirect, incidental, lost profits, special, consequential, punitive or exemplary damages, including, but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses (even if the Company has been advised of the possibility of such damages), resulting from: (i) the use or the inability to use the Services; (ii) the cost of procurement of substitute goods and services resulting from any goods, data, information or services purchased or obtained or messages received or transactions entered into through or from the Services; (iii) unauthorized access to or alteration of your transmissions or data; (iv) statements or conduct of any third party on the service; (v) or any other matter

relating to these Terms or the Services, whether as a breach of contract, tort (including negligence whether active or passive), or any other theory of liability.

In other words: choosing to use our Services does mean you are making a bet on us. If the bet does not work out, that's on you, not us. We do our best to be as safe a bet as possible through careful management of the business; investments in security, infrastructure, and talent. If you choose to use our Services, thank you for betting on us.

If you have a question about any of these Terms, please contact support at info@outreachbot.com.

Restricted purposes

When you use any of Outreachbot's Services, you acknowledge that you may not:

- Collect or extract information and/or user data from accounts which do not belong to you.
- Circumvent, disable, or otherwise interfere with security-related features of the Services.
- Trick, defraud, or mislead us or other users, including but not limited to making false reports or impersonating another user.
- Upload or transmit (or attempt to upload or to transmit) viruses or any type of malware, or information collection mechanism, including 1×1 pixels, web bugs, cookies, or other similar devices.
- Interfere with, disrupt, or create an undue burden on the Services or the networks or the Services connected.
- Harass, annoy, intimidate, or threaten others, or any of our employees engaged in providing any portion of the Services to you.
- Disparage, tarnish, or otherwise harm, in our opinion, us and/or the Services.
- Use the Services in a manner inconsistent with any applicable laws or regulations.

Accounts found to be in violation of any of the above are subject to cancellation without prior notice.

How to report abuse

Violations can be reported by emailing info@outreachbot.com and should include detailed information about the account, the content or behavior you are reporting, and how you found it, including URLs or screenshots. If you need a secure file transfer, let us know and we will send you a link. We will not disclose your identity to anyone associated with the reported account. For copyright cases, please see instructions on how to notify us about infringement claims.

Cancellation policy

We make it easy for you to cancel your account by emailing info@outreachbot.com

Our legal responsibility is to account owners, which means we cannot cancel an account at the request of anyone else. If for whatever reason you no longer know who the account owner is contact us. We will gladly reach out to any current account owners at the email addresses we have on file.

What happens when you cancel an account?

You won't be able to access your account once you cancel, so make sure you download everything you want to keep beforehand. If you have a paid account, you can cancel your subscription and keep using your account until your paid period expires. Then the account will be automatically canceled and will become inaccessible. You can also choose to cancel your account earlier.

We'll permanently delete the content in your account from our servers 30 days after cancellation, and from our backups within 60 days. Retrieving content for a single account from a backup isn't possible, so if you change your mind you'll need to do it within the first 30 days after cancellation. **Content can't be recovered once it has been permanently deleted.**

We won't bill you again once you cancel. We don't automatically prorate any unused time you may have left but if you haven't used your account in months or just started a new billing cycle for a fair refund. We'll treat you right.

Outreachbot-initiated cancellations

We may cancel accounts if they have been inactive for an extended period:

- For trial accounts:
    - For other services: 30 days after a trial has expired without being upgraded
- For frozen accounts: 180 days after being frozen due to billing failures
- For free accounts: after 365 days of inactivity

We also retain the right to suspend or terminate accounts for any reason at any time, as outlined in our Terms of Service. In practice, this generally means we will cancel your account without notice if we have evidence that you are using our products to engage in abusive behavior.

Use Restrictions

Restricted purposes

When you use any of Outreachbot's' Services, you acknowledge that you may not:

- Collect or extract information and/or user data from accounts which do not belong to you.
- Circumvent, disable, or otherwise interfere with security-related features of the Services.
- Trick, defraud, or mislead us or other users, including but not limited to making false reports or impersonating another user.
- Upload or transmit (or attempt to upload or to transmit) viruses or any type of malware, or information collection mechanism, including 1×1 pixels, web bugs, cookies, or other similar devices.
- Interfere with, disrupt, or create an undue burden on the Services or the networks or the Services connected.
- Harass, annoy, intimidate, or threaten others, or any of our employees engaged in providing any portion of the Services to you.
- Disparage, tarnish, or otherwise harm, in our opinion, us and/or the Services.
- Use the Services in a manner inconsistent with any applicable laws or regulations.

Accounts found to be in violation of any of the above are subject to cancellation without prior notice.

How to report abuse

Violations can be reported by emailing info@outreachbot.com and should include detailed information about the account, the content or behavior you are reporting, and how you found it, including URLs or screenshots. If you need a secure file transfer, let us know and we will send you a link. We will not disclose your identity to anyone associated with the reported account. For copyright cases, please see instructions on how to notify us about infringement claims.

Copyright Infringement Claims

Notification of Copyright Infringement Claims

Making original work is hard! As described in our Use Restrictions policy, you can't use Outreachbot products* to make or disseminate work that uses the intellectual property of others beyond the bounds of fair use.

Are you a copyright owner? Under the Digital Millennium Copyright Act (17 U.S.C. § 512), you have the right to notify us (Outreachbot) if you believe that an account user of any product we built and maintain has infringed on your work(s) as copyright owner. To be

effective, the notification of claimed infringement must be written. Please include the following information:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
- Identification of the copyrighted work(s) claimed to have been infringed. If there are multiple, please share a representative list of those works.
- A way for us to locate the material you believe is infringing the copyrighted work.
- Your name and contact information so that we can get back to you. Email address is preferred but a telephone number or mailing address works too.
- A statement that you, in good faith, believe that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
- A statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Digital Millennium Copyright Act ("DCMA") Counter-notifications

On the flip-side, if you believe your material has been removed in error, you can file a written counter-notification. Please include the following information:

- A physical or electronic signature, or the signature of the person authorized to act on your behalf.
- A description of the material that was removed.
- A description of where the material appeared in Outreachbot products prior to their removal.
- Your name and contact information so that we can get back to you. Email address is preferred but a telephone number or mailing address works too.
- A statement under penalty of perjury that you have a good faith belief that the material was removed or disabled as a result of mistake or misidentification.
- A statement that you consent to the jurisdiction of the Federal District Court for the judicial district in which your address is located, or if your address is outside of the United States, in Delaware (where Outreachbot is located).
- A statement that you will accept service of process from the person who filed the original DMCA notice or an agent of that person. (In other words, you've designated that person to receive documents on your behalf.)

Where to Send Notices

You can notify us of either copyright infringement claims or DCMA counter-notifications through either of the following channels:

By email: info@outreachbot.com

By mail: Outreachbot 1 Bluxome St 401 San Francisco CA 94107: Gil Pignol San Francisco CA 94107

**This policy and process applies to any product created and owned by Outreachbot*

A fair refund policy.

Bad refund policies are infuriating. You feel like the company is just trying to rip you off. We never want our customers to feel that way, so our refund policy is simple: If you're ever unhappy with our products* for any reason, just contact us and we'll take care of you.

Examples of full refunds we'd grant.

- If you were just charged for your next month of service but you meant to cancel, we're happy to refund that extra charge.
- If you forgot to cancel your account a couple months ago and you haven't used it since then, we'll give you a full refund for a few back months. No problem.
- If you tried one of our products for a couple months and you just weren't happy with it, you can have your money back.

Examples of partial refunds or credits we'd grant.

- If you forgot to cancel your account a year ago, and there's been activity on your account since then, we'll review your account usage and figure out a partial refund based on how many months you used it.
- If you upgraded your account a few months ago to a higher plan and kept using it in general but you didn't end up using the extra features, projects, or storage space, we'd consider applying a prorated credit towards future months.
- If we had extended downtime (multiple hours in a day, or multiple days in a month) or you emailed customer service and it took multiple days to get back to you, we'd issue a partial credit to your account.

Get in touch

At the end of the day, nearly everything on the edges comes down to a case-by-case basis. Send us a note and tell us what's up, and we'll work with you to make sure you're happy.

Security overview.

We protect your data.

All data are written to multiple disks instantly, backed up daily, and stored in multiple locations. Files that our customers upload are stored on servers that use modern techniques to remove bottlenecks and points of failure.

Your data are sent using HTTPS.

Whenever your data are in transit between you and us, everything is encrypted, and sent using HTTPS. Within our firewalled private networks, data may be transferred unencrypted.

Any files which you upload to us are stored and are encrypted at rest. Our application databases are generally not encrypted at rest — the information you add to the applications is active in our databases and subject to the same protection and monitoring as the rest of our systems. Our database backups are encrypted using GPG.

Full redundancy for all major systems.

Our servers — from power supplies to the internet connection to the air purifying systems — operate at full redundancy. Our systems are engineered to stay up even if multiple servers fail.

Sophisticated physical security.

Our state-of-the-art servers are protected by biometric locks and round-the-clock interior and exterior surveillance monitoring. Only authorized personnel have access to the data center. 24/7/365 onsite staff provides additional protection against unauthorized entry and security breaches.

Regularly-updated infrastructure.

Our software infrastructure is updated regularly with the latest security patches. Our products run on a dedicated network which is locked down with firewalls and carefully monitored. While perfect security is a moving target, we work with security researchers to keep up with the state-of-the-art in web security.

We protect your billing information.

All credit card transactions are processed using secure encryption—the same level of encryption used by leading banks. Card information is transmitted, stored, and processed securely on a PCI-Compliant network.

Constant monitoring

We have a team dedicated to maintaining your account's security on our systems and monitoring tools we've set up to alert us to any nefarious activity against our domains. To date, we've *never* had a data breach.

We also audit internal data access. If a Outreachbot employee wrongly accesses customer data, they will face penalties ranging from termination to prosecution. Again, to our knowledge, this hasn't happened.

We have processes and defenses in place to keep our streak of 0 data breaches going. But in the unfortunate circumstances someone malicious does successfully mount an attack, we will immediately notify all affected customers.

Have a concern? Need to report an incident?

Have you noticed abuse, misuse, an exploit, or experienced an incident with your account? Please visit our security response page for details on how to securely submit a report.

Security response

We appreciate your concern

Keeping customer data safe and secure is a huge responsibility and a top priority. We work hard to protect our customers from the latest threats. Your input and feedback on our security is always appreciated.

Reporting security problems

Report security vulnerabilities please email us as info@outreachbot.com We'll respond as soon as we can.

For other urgent or sensitive reports, please email us as info@outreachbot.com We'll respond as soon as we can.

For requests that aren't urgent or sensitive: , please email us as info@outreachbot.com

Tracking and disclosing security issues

We work with security researchers to keep up with the state-of-the-art in web security. Have you discovered a web security flaw that might impact our products? Please let us know. If you submit a report via info@outreachbot.com, here's what will happen:

- We'll acknowledge your report.
- We'll triage your report.
- We'll investigate the issue and determine how it impacts our products. We won't disclose issues until they've been fully investigated and patched, but we'll work with you to ensure we fully understand severity and impact.
- Once the issue is resolved, we'll post a security update along with thanks and credit for the discovery.

We ask for your patience while we also make sure other companies and their customers are protected. Either way, you'll always have a Outreachbot.com contact for your issue.

Thanks for working with us

We respect the time and talent that drives new discoveries in web security technology.

Privacy policy

The privacy of your data—and it is your data, not ours!—is a big deal to us. In this policy, we lay out: what data we collect and why; how your data is handled; and your rights with respect to your data. We promise we never sell your data: never have, never will.

This policy is split into sections. For your convenience, links to each of those sections is as follows:

This policy applies to our handling of information about site visitors, prospective customers, and customers and authorized users (in relation to their procurement of the services and management of their relationship with Outreachbot). We refer collectively to these categories of individuals as "you" throughout this policy.

However, this policy does not cover information about a customer's end users that Outreachbot receives from a customer, or otherwise processes on a customer's behalf, in connection with the services provided by Outreachbot to the customer pursuant to an applicable services agreement (including the content of messages of customer end users ("End User Communications")). Outreachbot processes End User Communications under the instructions of the relevant customer, which is the "data controller" or "business" (or occupies a similar role as defined in applicable privacy laws), as described in the applicable services agreement between such customer and Outreachbot. Outreachbot's obligations as a "data processor" or "service provider" with respect to such information are defined in such services agreement and applicable data protection addendum and are not made part of this policy.

If you are a customer's end user and you have questions about how your information is collected and processed through the services, please contact the organization who has provided your information to us for more information.

If you are a California resident, please click here to see our California Notice at Collection, which includes additional disclosures as required by California law.

What we collect and why

Our guiding principle is to collect only what we need. Here's what that means in practice:

Identity and access

When you sign up for a Outreachbot product, we ask for identifying information such as your name, email address, and maybe a company name. That's so you can personalize your new account, and we can send you product updates and other essential information. We may also send you optional surveys from time to time to help us understand how you use our products and to make improvements. With your consent, we will send you our newsletter and other updates. We sometimes also give you the option to add a profile picture that displays in our products.

We'll never sell your personal information to third parties, and we won't use your name or company in marketing statements without your permission either.

Billing information

If you sign up for a paid Outreachbot product, you will be asked to provide your payment information and billing address. Credit card information is submitted directly to our payment processor and doesn't hit Outreachbot servers. We store a record of the payment transaction, including the last 4 digits of the credit card number, for purposes of account history, invoicing, and billing support. We store your billing address so we can charge you for service, calculate any sales tax due, send you invoices, and detect fraudulent credit card transactions. We occasionally use aggregate billing information to guide our marketing efforts.

Product interactions

We store on our servers the content that you upload or receive or maintain in your Outreachbot product accounts. This is so you can use our products as intended. We keep this content as long as your account is active. If you delete your account, we'll delete the content within 60 days.

General Geolocation data

For most of our products, we log the full IP address used to sign up a product account and retain that for use in mitigating future spammy signups. We also log all account access by full IP address for security and fraud prevention purposes, and we keep this login data for as long as your product account is active.

Website interactions

We collect information about your browsing activity for analytics and statistical purposes such as conversion rate testing and experimenting with new product designs. This includes, for example, your browser and operating system versions, your IP address, which web pages you visited and how long they took to load, and which website referred you to us. If you have an account and are signed in, these web analytics data are tied to your IP address and user account until your account is no longer active. The web analytics we use are described further in the Advertising and Cookies section.

Anti-bot assessments

We use CAPTCHA across our applications to mitigate brute force logins and as a means of spam protection. We have a legitimate interest in protecting our apps and the broader Internet community from credential stuffing attacks and spam. When you log into your Outreachbot accounts and when you fill in certain forms, the CAPTCHA service evaluates various information (e.g., IP address, how long the visitor has been on the app, mouse movements) to try to detect if the activity is from an automated program instead of a human. The CAPTCHA service then provides Outreachbot with the spam score results; we do not have access to the evaluated information.

Advertising and Cookies

Outreachbot runs contextual ads on various third-party platforms such as Google, Reddit, and LinkedIn. Users who click on one of our ads will be sent to the Outreachbot marketing site. Where permissible under law, we may load an ad-company script on their browsers that sets a third-party cookie and sends information to the ad network to enable evaluation of the effectiveness of our ads, e.g., which ad they clicked and which keyword triggered the ad, and whether they performed certain actions such as clicking a button or submitting a form.

We also use persistent first-party cookies and some third-party cookies to store certain preferences, make it easier for you to use our applications, and perform A/B testing as well as support some analytics.

A cookie is a piece of text stored by your browser. It may help remember login information and site preferences. It might also collect information such as your browser type, operating system, web pages visited, duration of visit, content viewed, and other click-stream data. You can adjust cookie retention settings and accept or block individual cookies in your browser settings, although our apps won't work and other aspects of our service may not function properly if you turn cookies off.

Voluntary correspondence

When you email Outreachbot with a question or to ask for help, we keep that correspondence, including your email address, so that we have a history of past correspondence to reference if you reach out in the future.

We also store information you may volunteer, for example, written responses to surveys. If you agree to a customer interview, we may ask for your permission to

record the conversation for future reference or use. We will only do so with your express consent.

How we approach mobile app permissions

We offer optional desktop and mobile apps for some of our products. Because of how the platforms are designed, our apps typically must request your consent before accessing contacts, calendar, camera, and other privacy-sensitive features of your device. Consent is always optional and our apps will function without it, though some features may be unavailable. There are a few exceptions, for example:

- Our iOS apps will ask for permission to use push notifications upon first sign-in.
- Android apps do not require permission to send push notifications.

When we access or disclose your information

To provide products or services you've requested. We use some third-party subprocessors to help run our applications and provide the Services to you. You can view the third-party subprocessors we use for each of our products: We also use third-party processors for other business functions such as managing newsletter subscriptions, sending customer surveys, and providing our company storefront.

We may disclose your information at your direction if you integrate a third-party service into your use of our products. For example, we may allow you, at your option, to connect your email account to your account so that you can use to receive and respond to your email. Email that you receive and respond to through Outreachbot from your email address will be stored by both Outreachbot and Google and will be available to you from your Gmail account as well as your account.

No Outreachbot human looks at your content except for limited purposes with your express permission, for example, if an error occurs that stops an automated process from working and requires manual intervention to fix. These are rare cases, and when they happen, we look for root cause solutions as much as possible to avoid them recurring. We may also access your data if required in order to respond to legal process (see "When required under applicable law" below).

To exclude you from seeing our ads. Where permissible by law and if you have a Outreachbot account, we may disclose a one-way hash of your email address with ad companies to exclude you from seeing our ads.

To help you troubleshoot or squash a software bug, with your permission. If at any point we need to access your content to help you with a support case, we will ask for your consent before proceeding.

To investigate, prevent, or take action regarding restricted uses. Accessing a customer's account when investigating potential abuse is a measure of last resort. We want to protect the privacy and safety of both our customers and the people reporting issues to us, and we do our best to balance those responsibilities throughout the process. If we discover you are using our products for a restricted purpose, we will take action as necessary, including notifying appropriate authorities where warranted.

Aggregated and de-identified data. We may aggregate and/or de-identify information collected through the services. We may use de-identified or aggregated data for any purpose, including marketing or analytics.

When required under applicable law. Outreachbot is a U.S. company and all data infrastructure are located in the U.S.

- Requests for user data. Our policy is to not respond to government requests for user data unless we are compelled by legal process or in limited circumstances in the event of an emergency request. However, if U.S. law enforcement authorities have the necessary warrant, criminal subpoena, or court order requiring us to disclose data, we must comply. Likewise, we will only respond to requests from government authorities outside the U.S. if compelled by the U.S. government through procedures outlined in a mutual legal assistance treaty or agreement. It is Outreachbot' policy to notify affected users before we disclose data unless we are legally prohibited from doing so, and except in some emergency cases.

- Preservation requests. Similarly, Outreachbot' policy is to comply with requests to preserve data only if compelled by the U.S. Federal Stored Communications Act, 18 U.S.C. Section 2703(f), or by a properly served U.S. subpoena for civil matters. We do not disclose preserved data unless required by law or compelled by a court order that we choose not to appeal. Furthermore, unless we receive a proper warrant, court order, or subpoena before the required preservation period expires, we will destroy any preserved copies of customer data at the end of the preservation period.

- If we are audited by a tax authority, we may be required to disclose billing-related information. If that happens, we will disclose only the minimum needed, such as billing addresses and tax exemption information.

Finally, if Outreachbot is acquired by or merges with another company — we don't plan on that, but if it happens — we'll notify you well before any of your personal information is transferred or becomes subject to a different privacy policy.

Your rights with respect to your information

At Outreachbot, we strive to apply the same data rights to all customers, regardless of their location. Some of these rights include:

- **Right to Know.** You have the right to know what personal information is collected, used, shared or sold. We outline both the categories and specific bits of data we collect, as well as how they are used, in this privacy policy.
- **Right of Access.** This includes your right to access the personal information we gather about you, and your right to obtain information about the sharing, storage, security and processing of that information.
- **Right to Correction.** You have the right to request correction of your personal information.
- **Right to Erasure / "To Be Forgotten".** This is your right to request, subject to certain limitations under applicable law, that your personal information be erased from our possession and, by extension, from all of our service providers.

Fulfillment of some data deletion requests may prevent you from using Outreachbot services because our applications may then no longer work. In such cases, a data deletion request may result in closing your account.

- **Right to Complain.** You have the right to make a complaint regarding our handling of your personal information with the appropriate supervisory authority.
- **Right to Restrict Processing.** This is your right to request restriction of how and why your personal information is used or processed, including opting out of sale of your personal information. (Again: we never have and never will sell your personal data.)
- **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 have about you and the right to transmit it to another party.
- **Right to not Be Subject to Automated Decision-Making.** You have the right to object to and prevent any decision that could have a legal or similarly significant effect on you from being made solely based on automated processes. This right is limited if the decision is necessary for performance of any contract between you and us, is allowed by applicable law, or is based on your explicit consent.
- **Right to Non-Discrimination.** We do not 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 may, by virtue of your exercising those rights, prevent you from using our Services.

Many of these rights can be exercised by signing in and updating your account information. Please note that certain information may be exempt from such requests under applicable law. For example, we need to retain certain information in order to provide our services to you.

In some cases, we also need to take reasonable steps to verify your identity before responding to a request, which may include, at a minimum, depending on the sensitivity of the information you are requesting and the type of request you are making, verifying your name and email address. If we are unable to verify you, we may be unable to respond to your requests. If you have questions about exercising these rights or need assistance, please contact us at info@outreachbot.com or at Outreachbot, 1 Bluxome St 401 San Francisco CA USA. If an authorized agent is corresponding on your behalf, we will need written consent with a signature from the account holder before proceeding.

Depending on applicable law, you may have the right to appeal our decision to deny your request, if applicable. We will provide information about how to exercise that right in our response denying the request. You also have the right to lodge a complaint with a supervisory authority. If you are in the EU or UK, you can contact your data protection authority to file a complaint or learn more about local privacy laws.

How we secure your data

All data is encrypted via SSL/TLS when transmitted from our servers to your browser. The database backups are also encrypted. In addition, we go to great lengths to secure your data at rest.

What happens when you delete content in your product accounts

In many of our applications, we give you the option to trash content. Anything you trash in your product accounts while they are active will be kept in an accessible trash can for about 25 days (it varies a little by product). After that time, the trashed content cannot be accessed via the application and we are not able to retrieve it for you. The trashed content may remain on our active servers for another 30 days, and copies of the content may be held in backups of our application databases for up to another 30 days after that. Altogether, any content trashed in your product accounts should be purged from all of our systems and logs within 90 days.

If you choose to cancel your account, your content will become immediately inaccessible and should be purged from our systems in full within 60 days. This applies both for cases when an account owner directly cancels and for auto-canceled accounts. Please refer to our Cancellation policy for more details.

Data retention

We keep your information for the time necessary for the purposes for which it is processed. The length of time for which we retain information depends on the purposes for which we collected and use it and your choices, after which time we may delete and/or aggregate it. We may also retain and use this information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. Through this policy, we have provided specific retention periods for certain types of information.

Location of site and data

Our products and other web properties are operated in the United States. If you are located in the European Union, UK, or elsewhere outside of the United States, **please be aware that any information you provide to us will be transferred to and stored in the United States**. By using our websites or Services and/or providing us with your personal information, you consent to this transfer.

When transferring personal data from the EU

The European Data Protection Board (EDPB) has issued guidance that personal data transferred out of the EU must be treated with the same level of protection that is granted under EU privacy law. UK law provides similar safeguards for UK user data that is transferred out of the UK. Accordingly, Outreachbot has adopted a data processing addendum with Standard Contractual Clauses to help ensure this protection. Outreachbot' DPA is available here.

There are also a few ad hoc cases where EU personal data may be transferred to the U.S. in connection with Outreachbot operations, for instance, if an EU user signs up for our newsletter or participates in one of our surveys or buys swag from our company online store. Such transfers are only occasional and data is transferred under the Article 49(1)(b) derogation under GDPR and the UK version of GDPR.

Changes and questions

We may update this policy as needed to comply with relevant regulations and reflect any new practices. Whenever we make a significant change to our policies, we will refresh the date at the top of this page and take any other appropriate steps to notify users.

Have any questions, comments, or concerns about this privacy policy, your data, or your rights with respect to your information? Please get in touch by emailing us at info@usoutreach.com and we'll be happy to try to answer them!

How we handle abusive usage

We build our products to give teams a better way to work. We are proud of that purpose and trust that our customers use our products for appropriate endeavors.

Sometimes, though, we discover potential abusive usage as detailed in our Use Restrictions policy. When that happens, we investigate using the following guiding principles and process.

Guiding Principles

Human oversight

Who's "we", you ask? It's us: folks from the Outreachbot team. Our internal abuse oversight committee includes our executives, and representatives from multiple departments across the company. On rare occasions for particularly sensitive situations or if legally required, we may also seek counsel from external experts.

Balanced responsibilities

We have an obligation to protect the privacy and safety of both our customers and the people reporting issues to us. We do our best to balance those responsibilities throughout the process.

Focus on evidence

We base our decisions on the evidence available to us: what we see and hear account users say and do. We document what we observe and ask whether that observable evidence points to a restricted use.

Process

Every case goes through the same general process:

1. Discovery
2. Investigation
3. Decision, sometimes with right to an appeal

How do we discover potential abuse?

From our experience, we learn about potential abuse because:

- Someone alerts us. We give abuse reports our full care and attention. Our Support team also responds to every question or comment that comes in. If we notice anything in those emails that points to a violation, we will look into it.
- We notice an anomaly in our business operations monitoring. We monitor a range of things about our products, like signup volume and error rates of web requests. If we see something weird with those numbers, we get to the bottom of it.
- We stumble upon public web content that links an individual or organization to a Outreachbot product. We aren't scouring the Internet looking for those links, but if we do come across any, we check them out.

This list is not exhaustive; there are always edge cases. We will update the list if we find regular new avenues.

How do we investigate?

We focus on the evidence:

- Language and imagery used by users on the account
- Evidence of account users' power and/or ability to act on spoken claims
- Publicly available information about account users

We strive to balance privacy and safety for all those involved:

- We make every effort to complete our investigations without accessing a customer account. For instance, if there are screenshots or public documents available, we review those. We also consider whether it is appropriate to involve the account owner in a given investigation and seek additional evidence from them.
- As we review the evidence, we look for indications of existing negative impact. We also assess the severity of any potential negative impact, regardless of

intent. When relevant, we look for and follow available guidelines from expert institutions.
- If we cannot come to a fair assessment from the information available, we may decide to access a customer account without notice. We do not make this decision lightly. Customer privacy is a big deal to us and we only pursue this course of action if the evidence we have already is very concerning, but not definitive.

While some violations are flatly obvious, others are subjective, nuanced, and difficult to adjudicate. We give each case adequate time and attention, commensurate with the violation, criticality, and severity of the charge.

What happens if someone really broke the rules?

We will terminate an account without advance notice if there is evidence it is being used for a restricted purpose that has, is, or will cause severe harm. If applicable, we will also report the incident to the appropriate authorities.

For other cases, we'll take a case-by-case approach to clear things up.

Further, as a small, privately owned independent business that puts our values and conscience ahead of growth at all costs, we reserve the right to deny service to anyone we ultimately feel uncomfortable doing business with.

Can you appeal a decision?

If we terminate an account without notice, the decision is final.

For other cases, we will consider good faith appeals sent to info@outreachbot.com by the account owner within 14 calendar days.

DATA PROCESSING ADDENDUM

This Data Processing Addendum together with its Schedules and Appendices ("DPA") forms a part of the Outreachbot Terms of Service and Privacy Policy, both as updated from time to time, or other applicable agreement between Outreachbot LLC ("Outreachbot") and the

customer (“Customer”) identified in such agreement (“Agreement”) for the use of Outreachbot’ online services (“Services”). All capitalized terms not defined herein shall have the meaning set forth in the Agreement. To the extent of any conflict between this DPA, any previously executed data processing addendum, and the Agreement, this DPA will govern. In the event of any conflict or inconsistency between the body of this DPA on the one hand, and the UK Addendum and/or Standard Contractual Clauses (as applicable) on the other, the UK Addendum and/or Standard Contractual Clauses (as applicable) shall prevail. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, on behalf of Customer’s Authorized Affiliates. For the purposes of this DPA only, “Customer” shall include Customer and Authorized Affiliates. This DPA reflects the parties’ agreement with regard to the Processing of Personal Data. In the course of providing the Services to Customer pursuant to the Agreement, Outreachbot may process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data.

DATA PROCESSING TERMS

DEFINITIONS

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Authorized Affiliate” means any of Customer’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, (b) is permitted to use the Services pursuant to the Agreement between Customer and Outreachbot but has not signed its own Agreement with Outreachbot and is not a “Customer” as defined under the Agreement, and (c) qualifies as a Controller of Personal Data Processed by Outreachbot.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data, and includes “business” as defined in the CCPA.

“Customer Data” means what is described in the Outreachbot Privacy Policy, as “your data”, “your information” or similar terms.

“Data Protection Laws and Regulations” means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, to the extent applicable, laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom including the General Data Protection Regulation, Regulation (EU) 2016/679 (“GDPR”); the Swiss Federal Act on Data Protection (“FADP”); the United Kingdom Data Protection Act of 2018 (“UK GDPR”); and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. and associated regulations and amendments, including, when effective, the California Privacy Rights Act amendments (“CCPA”) and the privacy laws of other U.S. states (collectively, “U.S. Privacy Laws”).

“Data Subject” means the identified or identifiable person to whom Personal Data relates. “End Users” means Customer’s end users such as employees, contractors, “clients” as that term is used in Outreachbot, or others that Customer invites to use a Outreachbot Service via Customer’s account. 2

“Personal Data” means any information that is Customer Data and that relates to (i) an identified or identifiable natural person and/or (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data under applicable Data Protection Laws and Regulations).

“Processing” (including its various forms) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity that Processes Personal Data on behalf of the Controller and includes a “service provider” as defined under the CCPA.

“Security, Privacy and Architecture Documentation” means Outreachbot’s security overview and security whitepaper, Outreachbot’s Privacy Policy, as updated from time to time and accessible or other documentation made reasonably available by Outreachbot.

“Standard Contractual Clauses” means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, located at http://data.europa.eu/eli/dec_impl/2021/914/oj, and completed as set forth in Section 11 below.

“Subprocessor” means any Processor engaged by Outreachbot. “Supervisory Authority” means an independent public authority that is established by an EEA State pursuant to the GDPR, the UK’s Information Commissioner’s Office and/or the Swiss Federal Data Protection and Information Commissioner.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at https://ico.org.uk/media/fororganisations/documents/4019539/international-data-transfer-addendum.pdf).

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is either a Controller or Processor of Personal Data and Outreachbot is a Processor.

2.2 Customer’s Processing of Personal Data. Customer shall, in its use of the Services:

2.2.1 Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations;

2.2.2 have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquires Personal Data;

2.2.3 have provided adequate notices to, and obtained valid consents from, any Data Subjects relating to the Processing (including the disclosure) of Personal Data by Customer and, as applicable, to cross-border transfers of such Personal Data; and

2.2.4 shall not, by act or omission, cause Outreachbot to violate any Data Protection Laws and Regulations, or notices provided to or consents obtained from Data Subjects as result of Processing the Personal Data.

2.3 Outreachbot's Processing of Personal Data.
2.3.1 Outreachbot shall treat Personal Data as confidential information and shall only Process Personal Data: (1) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on behalf of Customer and in accordance with Customer's documented instructions; and (3) in compliance with Data Protection Laws and Regulations. This DPA and the Agreement are Customer's complete and final documented instructions to Outreachbot for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of the UK Addendum and/or Standard Contractual Clauses (as applicable), the following is deemed an instruction by the Customer to process Personal Data: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customer and/or its End Users in their use of the Services; and (iii) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement and this DPA.

2.3.2 The subject matter of Processing of Personal Data by Outreachbot is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1.

2.3.3 Without prejudice to section 2.3.1, Outreachbot shall: i. Not "sell" Personal Data or "share" Personal Data for purposes of "cross-context behavioral advertising" or "targeted advertising" as such terms are defined under U.S. Privacy Laws; ii. Not attempt to (a) re-identify any pseudonymized, anonymized, aggregate, or deidentified Personal Data or (b) link or otherwise create a relationship between Customer Data and any other data, without Customer's express authorization; iii. Not retain, use, or disclose Personal Data outside of the direct business relationship between Customer and Outreachbot; iv. Comply with any applicable restrictions under U.S. Privacy Laws on combining Personal Data with personal data that Outreachbot receives from, or on behalf of, another person or persons, or that the Outreachbot collects from any interaction between it and a data subject; and v. Immediately notify Customer if Outreachbot determines that (a) it can no longer meet its obligations under this DPA or Data Protection Laws and Regulations; (b) it has breached this DPA; or (c) in Outreachbot's opinion, an instruction from Customer infringes Data Protection Laws and Regulations.

2.3.4 Outreachbot shall promptly notify Customer of any government requests for access to or information about Outreachbot's Processing of Personal Data on Customer's behalf unless prohibited by Data Protection Laws and Regulations. Outreachbot will provide Customer with reasonable cooperation and assistance in relation to any such request. If Outreachbot is prohibited by applicable Data Protection Laws and Regulations from disclosing the details of a government request to Customer, Outreachbot shall inform Customer that it can no longer comply with Customer's instructions under this DPA without providing more details and await Customer's further instructions. Outreachbot shall use all available legal mechanisms to challenge any demands for data access through national security process that it receives, as well as any non-disclosure provisions attached thereto.

2.3.5 Outreachbot shall provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Protection Laws and Regulations, and at 4 Customer's reasonable expense.

2.3.6 Outreachbot shall provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Outreachbot under Data Protection Laws and Regulations to consult with a regulatory authority in relation to Outreachbot' Processing or proposed Processing of Personal Data.

2.3.7 Outreachbot certifies that it understands its obligations under this DPA (including without limitation the restrictions under Section 2) and that it will comply with them.

3.DATA SUBJECT REQUESTS

Outreachbot shall, to the extent legally permitted, promptly notify Customer if Outreachbot receives a request from a Data Subject to exercise the Data Subject's rights related to Personal Data under Data Protection Laws and Regulations, including the right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability; to object to the Processing, or to assert its right not to be subject to an automated individual decision making process ("Data Subject Request"). Taking into account the nature of the Processing, Outreachbot shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Outreachbot shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Outreachbot is legally permitted to do so and the response is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Outreachbot's provision of such assistance.

4. Outreachbot PERSONNEL

4.1 Confidentiality. Outreachbot shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality

agreements. Outreachbot shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. Outreachbot shall take commercially reasonable steps to ensure the reliability of any Outreachbot personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Outreachbot shall ensure that Outreachbot's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 Questions. For questions about this DPA or any other privacy matters, please send an email to info@outreachbot.com.

5. SUBPROCESSORS

5.1 Appointment of Subprocessors. Customer acknowledges and agrees that Outreachbot may engage thirdparty Subprocessors in connection with the provision of the Services. Outreachbot has entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data, to the extent such is applicable to the nature of the Services provided by such Subprocessor.

5.2 List of Current Subprocessors and Notification of New Subprocessors. Outreachbot shall make available to Customer the current list of Subprocessors for the Outreachbot Services on Outreachbot's website. Outreachbot shall provide notification to the Customer of a new Subprocessor(s) before authorizing any new Subprocessor(s) to Process Personal Data in connection with the provision of the applicable 5 Services. Customers must subscribe to the Outreachbot Subprocessor Github page for notification of Subprocessor changes.

5.3 Objection Right for New Subprocessors. Customer may object to Outreachbot's use of a new Subprocessor by notifying Outreachbot promptly in writing within ten (10) business days after receipt of Outreachbot's notice of a new Subprocessor in accordance with Section 5.2. In the event Customer objects to a new Subprocessor, Outreachbot may, at its option, use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the new Subprocessor without unreasonably burdening the Customer. If Outreachbot is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate with written notice to Outreachbot the applicable Agreement solely with respect to Services that cannot be provided by Outreachbot without use of the new Subprocessor. As of the effective date of termination, Outreachbot will refund Customer any prepaid fees such terminated Services covering the remainder of the term and will not penalize Customer for such termination.

6. SECURITY

6.1 Controls for the Protection of Personal Data. Outreachbot shall maintain appropriate technical and organizational measures to protect the security (including protection against unauthorized or unlawful Processing; accidental or unlawful destruction, loss or alteration or damage; or unauthorized disclosure of, or access to, Personal Data), confidentiality, and integrity of Personal Data, as set forth in the Security, Privacy and Architecture

Documentation. Outreachbot will not materially decrease the overall security of the Services during a subscription term.

6.2 Third-Party Certifications and Audits. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Outreachbot shall make available to Customer a copy of Outreachbot's then most recent third-party audits or certifications, as applicable; provided, however, that this provision shall not apply if Customer or Customer's independent, thirdparty auditor is a competitor of Outreachbot.

6.3 Unauthorized Processing of Personal Data. Customer retains the right to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Personal Data, including any Processing of Personal Data not authorized in this DPA.

7.PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Outreachbot maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and the Agreement. Outreachbot shall notify Customer without undue delay, and in compliance with Data Protection Laws and Regulations, after becoming aware of the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed by Outreachbot or its Subprocessors (a "Personal Data Incident"). Outreachbot shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Outreachbot deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Outreachbot's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's End Users.

8. RETURN AND DELETION OF PERSONAL DATA Upon termination of the Agreement, Outreachbot shall return Personal Data to Customer and, to the extent allowed by applicable law, delete Personal Data in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation.

9. AUTHORIZED AFFILIATES 6

9.1 Contractual Relationship. Each Authorized Affiliate agrees to be bound by the terms of this DPA and, to the extent applicable, the Agreement. Further, all access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement, and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement by Customer entering into this DPA, and is only a party to the DPA.

9.2 Communication. Customer shall remain responsible for coordinating all communication with Outreachbot under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Outreachbot, it shall, to the extent required under applicable Data Protection Laws

and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require that the Authorized Affiliate exercise a right or seek any remedy under this DPA against Outreachbot directly by itself, the parties agree that (a) only Customer shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and that (b) Customer shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below), not separately for each Authorized Affiliate individually.

9.3.2 The parties agree that Customer shall, when carrying out an on-site audit of the procedures relevant to protecting Personal Data, take all reasonable measures to limit any impact on Outreachbot and its Subprocessors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

To the extent permitted under applicable Data Protection Laws and Regulations, each party's and all of its Affiliates' liability arising out of or related to this DPA and all DPAs between Authorized Affiliates and Outreachbot, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability set forth in the Agreement, and such limitations apply to the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Outreachbot's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11. INTERNATIONAL DATA TRANSFERS

11.1 Subject to the additional terms in Schedule 1, Outreachbot makes available the Standard Contractual Clauses and the UK Addendum, which shall apply to any transfers of Personal Data under this DPA from the European Economic Area and/or their member states and Switzerland, and the United Kingdom, respectively, to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are made in connection with the Processing of Personal Data under the DPA and are subject to such Data Protection Laws and Regulations.

11.2 To the extent legally required, by signing the Agreement, Customer and Outreachbot are deemed to have signed the Standard Contractual Clauses, which form part of this DPA and (except as described in Section 11.4 and 11.5 below) will be deemed completed as follows:

11.2.1 Module 2 of the Standard Contractual Clauses applies to transfers of Personal Data from Customer (as a controller) to Outreachbot (as a processor) and Module 3 of the Standard Contractual Clauses applies to transfers of Personal Data from Customer (as a processor) to Outreachbot (as a processor); 7 11.2.2 Clause 7 (the optional docking clause) is included;

11.2.3 Under Clause 9 (Use of sub-processors), the Parties select Option 2 (General written authorization);

11.2.4 Under Clause 11 (Redress), the optional language requiring that Data Subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

11.2.5 Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the laws of Ireland;

11.2.6 Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;

11.2.7 Annex I(A) and I(B) (List of Parties) is completed as set forth in Schedule 1;

11.2.8 Under Annex I(C) (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission;

11.2.9 Annex II (Technical and organizational measures) is completed with Schedule 1 of this DPA; and 11.2.10 Annex III (List of subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9.

11.3 With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction or Switzerland) governs the international nature of the transfer, the UK Addendum forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK Addendum. Undefined capitalized terms used in this provision shall mean the definitions in the UK Addendum. For purposes of the UK Addendum, they shall be deemed completed as follows: (a) the Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer; (b) the Key Contacts shall be the contacts set forth in Schedule 1; (c) the Approved Standard Contractual Clauses referenced in Table 2 shall be the Standard Contractual Clauses as executed by the Parties; (d) either Party may end this DPA as set out in Section 19 of the UK Addendum; and (e) by entering into the Agreement, the Parties are deemed to be signing the UK Addendum.

11.4 For transfers of Personal Data that are subject to the FADP, the Standard Contractual Clauses form part of this DPA as set forth in Section 7(b) of this DPA, but with the following differences to the extent required by the FADP: (1) references to the GDPR in the Standard Contractual Clauses are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (2) references to personal data in the Standard Contractual Clauses also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; (3) the term "member state" in Standard Contractual Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses; and (4) the relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the

GDPR), or both such Commissioner and the supervisory authority identified in the Standard Contractual Clauses (where the FADP and GDPR apply, respectively)

11.5 Copies of Subprocessor Agreements. The parties agree that copies of the Subprocessor agreements that must be provided by Outreachbot to Customer pursuant to the applicable Standard Contractual Clauses or Controller to Processor Clauses, or Processor to Processor Clauses may have all commercial information or clauses unrelated to the applicable Standard Contractual Clauses, Controller to Processor Clauses, or Processor to Processor Clauses removed by Outreachbot beforehand; and, that such copies will be provided by Outreachbot, in a manner to be determined in its discretion, only upon request by Customer.

11.6 Processor to Processor Clauses. For purposes of the Processor to Processor Clauses, Customer agrees 8 that it is unlikely that Outreachbot will know the identity of Customer's Controller(s) because Outreachbot does not have a direct relationship with such Controller(s). Therefore, Customer will fulfill any and all of Outreachbot's obligations to Customer's Controller(s) under the Processor to Processor Clauses.

11.7 Audits and Certifications. The parties agree that the audits described in the UK Addendum and/or Standard Contractual Clauses (as applicable) shall be carried out in accordance with Section 6.2 of the DPA. 11.8 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in the UK Addendum and/or Standard Contractual Clauses (as applicable) shall be provided by Outreachbot to Customer only upon Customer's request. 9

SCHEDULE 1 ANNEX I A. LIST OF PARTIES

Data exporter(s): Name: The entity identified as Customer in the DPA or such other agreement between Outreachbot and Customer Address: The Address for the Customer associated with the Outreachbot account Contact person’s name, position and contact details: The contact details associated with the Outreachbot Account Activities relevant to the data transferred under these Clauses: The activities specified in the DPA Signature and date: By using Outreachbot’s services to transfer data to Third Countries, the exporter will be deemed to have signed Annex 1 Role (controller/processor): Controller, or in some instances Processor

Data importer(s): Name: Outreachbot LLC Address: 1 Bluxome St 401 San Francisco CA USA Contact person’s name, position and contact details: Gil Pignol, gil@outreachbot.com

Activities relevant to the data transferred under these Clauses: Outreachbot is a cloud- based software-as-aservice provider of collaboration and communication software which processes personal data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and Outreachbot. Signature and date: By processing the data exporter’s data on data exporter’s instructions, the data importer will be deemed to have signed this Annex I Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER Categories of data subjects whose personal data is transferred Data exporter and/or data subjects (as directed by data exporter), may submit personal data to the Services concerning the following categories of data subjects: • Prospects, customers business partners and vendors (who are natural persons) of data exporter; • Employees or contact persons of data exporter’s prospects, customers, business

partners and vendors; • Employees, agents, advisors, independent contractors, members and/or freelancers of data exporter; and/or • Other categories of data subjects as expressly determined by the data exporter. Categories of personal data transferred Data exporter and/or data subjects (as directed by data exporter) may submit personal data to the Services, the type, extent and detail of which is determined and controlled by the data exporter and/or the data subject in its sole discretion. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions 10 (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. Data exporter and/or data subjects (as directed by data exporter) may submit Sensitive Data to the Services, the type, extent and detail of which is determined and controlled by the data exporter and/or the data subject in its sole discretion. Outreachbot takes the security and privacy of data very seriously. The restrictions and safeguards that apply to all Personal Data, including any Sensitive Data, can be found in Outreachbot's Privacy Policy, as updated from time to time and accessible at https://Outreachbot.com/about/policies/privacy; security policies, as updated from time to time and accessible at https://Outreachbot.com/about/policies/security and
https://Outreachbot.com/about/policies/security/Outreachbot%20Security%20Overview.pdf, and HEY's security overview, as updated from time to time and accessible at https://www.hey.com/security/. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). Data exporter and/or data subjects (as directed by data exporter) may submit personal data to the Services either once, or on a continuous basis (for example by making changes to personal data) as determined and controlled by the data exporter and/or the data subject in its sole discretion. Nature of the processing Outreachbot processes personal data only as necessary to perform the Services and only performs the type(s) of processing as instructed by the data exporter and/or data subject and only pursuant to the Agreement, the DPA and these Clauses. Purpose(s) of the data transfer and further processing The purposes of the processing are determined solely by the data exporter and/or data subject in its sole discretion. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period Subject to any other terms allowing or requiring longer retention, and subject to Outreachbot's normal data retention policies, Outreachbot only processes personal data for the duration of the Agreement, unless the data is deleted prior thereto by the data exporter and/or data subject. For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing Outreachbot transfers Personal Data to Sub-processors as set forth in Outreachbot's Privacy Policy.

C. COMPETENT SUPERVISORY AUTHORITY Identify the competent supervisory authority/ies in accordance with Clause 13 The competent supervisory authority will be determined in accordance with the GDPR and where possible, will be the Irish Data Protection Commissioner.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The various measures we take to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons, can be found in Outreachbot's Privacy Policy, as updated from

time to time and accessible in this document; security policies, as updated from time to time and accessible in this document11 Outreachbot establishes data processing agreements with all of its sub-processors that handle personal data, which require those sub-processors to adhere to the same, if not more stringent requirements, as Outreachbot.

California Resident Notice at Collection

If you are a California resident, the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 ("**CCPA**"), requires us to provide some additional information to California residents. This Section only applies to you if you are a California resident, although please note that this information and the rights afforded herein are the same as offered to our other users in our main Privacy Policy. This Section does not apply to personal information we collect from our employees and job applicants in their capacity as employees and job applicants, as such information practices are described in separate policies.

The following chart details these activities:

Category of personal information	Purposes of use	Categories of Third Parties to Which We Discloses this Personal Information	Categories of Third Parties to Which We "Share" and "Sell" this Personal Information for Advertising/ Analytics Purposes
Contact information (such as your full name, phone number, email address)	Provide the Services; Communicate with you; Analyze use of and improve the services; With your consent; Comply with law or defend our legal rights; Security/fraud prevention	Affiliated entities; Service providers; Entities for legal purposes	We do not share/sell
Customer service interaction information (including optional surveys	Provide the Services; Communicate with you; Analyze use of and improve the services; With your	Affiliated entities; Service providers;	We do not share/sell

Category of personal information	Purposes of use	Categories of Third Parties to Which We Discloses this Personal Information	Categories of Third Parties to Which We "Share" and "Sell" this Personal Information for Advertising/ Analytics Purposes
and when you ask for help)	consent; Comply with law or defend our legal rights; Security/fraud prevention	Entities for legal purposes	
Product interaction information	Provide the Services; Communicate with you; Analyze use of and improve the services; With your consent; Comply with law or defend our legal rights; Security/fraud prevention	Affiliated entities; Service providers; Entities for legal purposes	We do not share/sell
Internet network and device information (such as mobile device information, IP address, and information about your interaction with the services)	Provide the Services; Analyze use of and improve the services; With your consent; Comply with law or defend our legal rights; Security/fraud prevention	Affiliated entities; Service providers; Entities for legal purposes;	We do not share/sell
Login information (such as your username and password)	Provide the Services; Comply with law or defend our legal rights; Security/fraud prevention; Comply with law or defend our legal rights	Affiliated entities; Service providers; Entities for legal purposes	We do not share/sell

Category of personal information	Purposes of use	Categories of Third Parties to Which We Discloses this Personal Information	Categories of Third Parties to Which We "Share" and "Sell" this Personal Information for Advertising/ Analytics Purposes
Professional or employment information (such as the name and address of the company you work for and your title)	Provide the Services; Communicate with you; Analyze use of and improve the services; With your consent; Comply with law or defend our legal rights; Security/fraud prevention	Affiliated entities; Service providers; Entities for legal purposes;	We do not share/sell
Other information (any other information you choose to provide directly to us, including optional profile photos)	Provide the Services; Communicate with you; Analyze use of and improve the services; With your consent; Comply with law or defend our legal rights; Security/fraud prevention	Affiliated entities; Service providers; Entities for legal purposes;	We do not sell/share

For more information about each category of personal information, purpose of use, and third parties to which we disclose personal information, please see the "What we collect and why," and "When we access or disclose you information" sections of our Privacy Policy.

Your Choices Regarding "Sharing" and "Selling": You have the right to opt out of our sale/sharing of your personal information for purposes of online analytics and advertising. Currently, we do not sell or share your data as defined by the CCPA and we have not done so over the past 12 months from the effective date of this Privacy Policy.

Other CCPA Rights. If we ever offer any financial incentives in exchange for your personal information, we will provide you with appropriate information about such incentives.

The CCPA also allows you to limit the use or disclosure of your "sensitive personal information" (as defined in the CCPA) if your sensitive personal information is used for certain purposes. Please note that we do not use or disclose sensitive personal

information other than for business purposes for which you cannot opt out under the CCPA.

Please see the “Your rights with respect to your information” section of our Policy above for information about the additional rights you have with respect to your personal information under California law and how to exercise them.

Retention of Your Personal Information. Please see the “Retention Of Your Information” section belowof our Privacy Policy for more information.

Shine the Light Disclosure

The California "Shine the Light" law gives residents of California the right under certain circumstances to request information from us regarding the manner in which we disclose certain categories of personal information (as defined in the Shine the Light law) with third parties for their direct marketing purposes. We currently do not disclose your personal information to third parties for their own direct marketing purposes.