Terms of Service

Effective Date: As of the date indicated in the Order under GSA Schedule Contracts.

Here are the ground rules if you're using our stuff. The following Terms of Service ("Terms," "Agreement") govern your use of DeleteMe, a service of Abine, Inc.

DeleteMe helps protect your privacy. Our DeleteMe service allows for the management of personal information and control of how other websites and businesses display such personal information. These Terms of Service describe the terms and conditions on which Abine provides the DeleteMe service to you but provisions regarding specific products or services apply only to the extent you have purchased, accessed, or used such products or services. For more information about how the DeleteMe service works, please visit our Frequently Asked Questions.

Legal policies can be tedious, but please read up. We'll strive to make our policies understandable. READ THIS AGREEMENT CAREFULLY. IF YOU ACCEPT THIS AGREEMENT BY EXECUTING THIS AGREEMENT OR A WRITTEN ORDER FOR USE OF THETHE DELETEME SERVICE OR APPLICATION, YOU ARE ENTERING INTO THIS AGREEMENT WITH ABINE. THIS IS A LEGALLY BINDING AGREEMENT. If you don't agree to these terms and conditions, you aren't permitted to use the DeleteMe services, our apps, or our website.

Things could change. We may non-materially amend or terminate any terms of this Agreement at any time and such non-material amendment or termination will be effective at the time we post the revised terms on the site. We'll strive to make these terms understandable. You can tell when we last revised this agreement was by looking at the "last updated" date at the top of this Agreement. Your continued use of the site or services after we've posted non-materially revised terms signifies your acceptance of the revised terms.

DeleteMe Users

There are two types of users of DeleteMe (collectively, "DeleteMe Users"). "Individual Users" are users who register an account to use and access features of DeleteMe that they purchase for themselves or who have a DeleteMe account purchased or gifted to them by another individual. "Business Users" are registered account users who's DeleteMe membership has been purchased by an Organization. "Organization" or "Organizations" means businesses and entities, (including private, public, government, and non-profit), that have entered into an Abine subscription agreement and subscribe with us to use and access DeleteMe for data removal services for their business. Business Users may also include Organization administrators who have access to certain features only available to an Organization (e.g., DeleteMe Privacy Center). Certain features of DeleteMe are only available to Enterprise Users and Organizations. Except as outlined below and in our Privacy Policy, the Terms apply equally to Individual Users and Enterprise Users.

Using DeleteMe – All DeleteMe Users

Except as otherwise described in these Terms or by a separate subscription agreement, if applicable, the following applies to all DeleteMe Users:

Tell the truth. You agree that all the information you're submitting to DeleteMe in connection with the services is and will be true and about you, not someone else. If you provide any information that is or that we suspect is untrue, inaccurate, not current or incomplete, Abine has the right to suspend or terminate your subscription in accordance with the Disputes Clause (Contract Disputes Act) and refuse any and all current or future use of your subscription.

Your data is yours. You retain ownership over all the personal information that you submit to the DeleteMe service, and Abine will never sell it. To fulfil your opt-out requests, we have to send your information to data brokers, which necessarily requires sharing your data with them. We can't control how these third-party data brokers will treat your personal information, although it is only provided to them so they can opt you out of their public databases.

Adults only. This service is meant to be used by adults only (18+) for themselves, or on behalf of a minor for whom they are the parent or legal guardian.

We'll try hard. DeleteMe allows subscribers like you to request that third party websites, such as data brokers and information aggregators, remove or suppress your personal information from their websites. You recognize that DeleteMe will use good faith, reasonable efforts to help you submit these opt-out requests, but that we cannot guarantee that third parties will honor the requests or remove your data.

It's unlikely, but bad things could happen. You acknowledge that your use of the DeleteMe service may have unintended consequences, possibly including direct, special, indirect, consequential and other damages, and you agree that you won't hold Abine liable for these consequences. (In English, not legalese: let's say that you have a long-lost brother who's looking for you via Intelius. Because we deleted you from Intelius, it takes him much longer to find you. You agree that you won't sue us because you lost the opportunity to spend more time with your brother.) Also, because lawyers often make a lot of clever arguments, you agree regardless of any claim you or lawyer comes up with the most you could ever recover in any claim brought by you against Abine is the total amount of fees you actually paid to Abine over the entire time you used the DeleteMe service. The foregoing limitation of liability shall not apply to (1) Licensor's fraud, gross negligence or willful misconduct; or (2) for any other matter for which liability cannot be excluded by law.

Reserved.

You're letting us do the work of removing your personal info from data broker websites. You grant Abine a Limited Power of Attorney to act on your behalf for the purposes of performing the DeleteMe service to control your personal information online, including submitting opt-out requests to and communicating with third-party websites like data brokers or aggregators or other parties who have control over this content, signing opt-out documents, creating accounts for you, and any other action Abine reasonably deems necessary to remove, suppress, or opt-out your personal information from unwanted sources in fulfillment of your order. This Limited Power of Attorney will remain in full force and effect until you cancel your service with Abine.

Data brokers change, so DeleteMe might change too. You acknowledge that DeleteMe's removal list depends on the listed websites' opt-out procedures and business practices and thus is subject to change. DeleteMe will not remove all of your information from the Internet. DeleteMe warrants that the DeleteMe service, content and site will days from the date of your receipt, perform substantially in accordance with DeleteMe service, content and site written materials accompanying it. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, As such, the DeleteMe service, content and site are provided on an "as is" basis, without warranties of any kind, either express or implied, including, without limitation, implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Consistent with what we stated above regarding damages, you agree that in any event, Abine's liability is limited to fees you actually paid to Abine.

If something crazy happens, it's not our fault. In accordance with GSAR Clause 552.212-4(f), You acknowledge that Abine will not be liable for any failure to comply with these Terms to the extent that such failure arises from factors outside Abine's reasonable control, like natural disasters.

Your Privacy

Privacy is key. Abine is dedicated to consumer privacy rights and operates the DeleteMe service under our **privacy policy** attached hereto.

Your Organization may have some obligations. Organizations using DeleteMe who are located in Europe, and are subject to the General Data Protection Regulation ("GDPR"), act as data controller with DeleteMe as their data processor. Our Organization customers must comply with applicable data protection laws, e.g., gathering consent from employees in a documented form where required by law. Abine is not liable for any unlawful processing or data sharing that occurs as a result of, for example, missing consent(s) or other non-compliance with the applicable data protection laws.

We urge you to read our **privacy policy** now and revisit occasionally because we may update it. We'll strive to make our policies understandable.

Your employer may have some obligations. Companies and other organizations who purchase DeleteMe, are located in Europe, and are subject to the General Data Protection

Regulation (GDPR), act as Data Controller with Abine, Inc. as their Data Processor. Our clients must comply with applicable data protection laws. For example they must gather consent from their employees or other end users in a documented form where required by law. Abine is not liable for any unlawful processing or data sharing that occurs as a result of missing consents or other non-compliance with the applicable data protection laws. If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

Please don't steal our stuff. All the text, images, marks, logos, compilations (meaning the collection, arrangement, and assembly of information) and other content on Abine's website ("Site Content"), and all software embodied in Abine's website, applications, or otherwise ("Software") used by to deliver the Services is proprietary to us. Except as otherwise expressly permitted by these Terms, any use, redistribution, sale, decompilation, reverse engineering, disassembly, translation, or other reduction of such software to human-readable form is prohibited. The text marks "ABINE," "ONLINE PRIVACY STARTS HERE," "DELETEME," "DONOTTRACKME," and "MASKME," as well as their associated logos, are our trademarks, and you may not use them in connection with any service or products other than those we provide in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Abine (although we're happy to have you use our Site Content for noncommercial, educational, or news-related use if you properly attribute it to us). Any use of such marks will apply to the benefit of their respective owners.

Use our tools and services for good, not evil, or we'll kick you out. We don't allow our Site or Services to be used for illegal activities or activities that we find improper for any reason whatsoever. We reserve the right to take preventative or corrective actions to protect ourselves and our users from anyone's unacceptable use. Your failure to comply with our Terms may result in us terminating your access to and use of our site and services in accordance with the Disputes Clause (Contract Disputes Act). You are not to:

- Impersonate anyone, falsely state or otherwise misrepresent your affiliation with any person or entity, or knowingly provide any fraudulent, misleading, or inaccurate information;
- Defame, abuse, harass, stalk, threaten, or otherwise violate others' rights, including without limitation others' privacy rights or rights of publicity;
- Access or use (or attempt to access or use) another user's account without permission;
- Transmit any software or materials that contain any viruses, worms, trojan horses, defects, or other items or computer code of a destructive nature;
- Modify, adapt, sublicense, translate, sell, reverse engineer, decompile, or disassemble any portion of the site or services;
- "Frame" or "mirror" any portion of the Site or Services;

- Use any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index, data mine, or in any way reproduce or circumvent the navigational structure or presentation of our site or services;
- Harvest or collect any other users' information from the site or our services;
- Use our site or services for any illegal activity; or
- Probe, scan or test the vulnerability of our site or services, breach their security or authentication measures, or take any action that imposes an unreasonable or disproportionately large load on our site infrastructure.

When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, DeleteMe shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer

Individual Users

We'll charge you for your subscription. You acknowledge that you're registering for a recurring subscription and will be automatically billed at the end of the subscription billing cycle for the annual period from the effective date of the subscription the anniversary date of the subscription.

You have the right to cancel your DeleteMe subscription at any time, for any reason, and can do so by emailing us at **support@joindeleteme.com** or calling us at 833-335-3836. You are entitled to a full refund if you cancel before your first DeleteMe Privacy Report. If you cancel anytime after your first DeleteMe Privacy Report, you are entitled to a prorated refund based on the time remaining in your DeleteMe subscription. Upon canceling your DeleteMe subscription, Abine will cease any future billing. This refund policy does not apply if we've terminated your account for misuse outlined in this Agreement. Any termination of your use of the DeleteMe service, whether initiated by you or by Abine, won't affect any of your or Abine's rights and obligations under these Terms that have arisen before the effective date of such termination.

Governing law. This Agreement shall be governed by the Federal law of the United States. Finally, you won't ever use our site or services in violation of U.S. export laws or regulations.

Business Users

DeleteMe Subscription Agreement. If you enrolled in our DeleteMe service and your Organization pays for your DeleteMe membership, payment terms for your use of the DeleteMe service is governed under the subscription agreement your Organization has entered into with Abine. Contact **sales@joindeleteme.com** for help or further information.

Cancellation of Your Service. You have a right to terminate your DeleteMe service, at any time, for any reason, and can do so by emailing us at **support@joindeleteme.com** or calling us at 833-335-3836.

DeleteMe Business Subscription Purchase Agreement

This BUSINESS SUBSCRIPTION PURCHASE AGREEMENT ("Agreement") is entered into by and between Abine, Inc. dba DeleteMe ("DeleteMe") and the entity named on the signature line below ("Buyer"), (individually, "the Party", jointly, "the Parties"). This Agreement governs access to DeleteMe's Software As A Service software and bundled services (together, "the Services"), and becomes effective upon mutual execution ("Effective Date").

Buyer and DeleteMe agree as follows:

1. Order: Buyer agrees to purchase subscriptions ("Subscriptions") from DeleteMe for the grant of a non-exclusive, non-transferable right to access and use the Services during the Term, solely for use by Authorized Users (as defined below) in accordance with the terms and conditions herein and as provided in accordance with any applicable document provisioning the Services (the "Order Form"). Buyer is restricted from making copies of on-premise software. Additionally, DeleteMe does not grant Buyer IP rights in DeleteMe's Software As A Service software. Buyer may purchase additional Subscriptions using an Order Form or other similarly accepted or executed document. Any additional licenses purchased during an active Subscription Term shall be co-termed with the original Subscription Term and shall expire on the same end date as the original Subscription unless otherwise agreed in writing by the parties. Fees for such additional licenses shall be prorated based on the remaining time in the Subscription Term. Buyer is responsible for determining to whom Subscriptions are assigned. Subscriptions are non-transferable, except to the extent that DeleteMe permits reassignment of seats under its then-current Subscription features. "Authorized User(s)" means Buyer's employees, consultants, contractors, and agents (i) who are authorized by Buyer to access and use the Services under the rights granted to Buyer pursuant to this Agreement and (ii) for whom access to the Services has been purchased as Subscriptions through (a) an applicable Order Form or (b) similarly accepted or executed document. "Subscription Term" means the period during which Buyer is authorized to access and use the Services under a specific Order. Each Subscription Term will begin on the Order Effective Date and continue for the duration specified in the Order, subject to renewal or termination as provided in this Agreement.

2. Services. DeleteMe agrees to provide Buyer the Services as identified in a) this Agreement, b) any additional Order Form and c) as designated by the Buyer or an Authorized User (jointly, the "Business Purpose"). Services may be updated from time to time and will be accessed subject to DeleteMe's Terms of Service attached hereto and at (https://privacy.joindeleteme.com/policies?name=terms-of-service)..

3. Data

3.1. Confidential Information. "Confidential Information" means all data and material provided by a Party ("Disclosing Party") disclosed to the other Party ("Receiving Party"), that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including the Services, business marketing plans, technology technical information, product designs, and business processes. Confidential Information shall not include End User Information (as defined below) nor information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (iii) was independently developed by the Receiving Party without breach of any obligation owed to the Disclosing Party; or (iv) is received from a third party without breach of any obligation owed to the Disclosing Party. The Receiving Party shall not disclose or use any Confidential Information of the Disclosing Party for any purpose outside of the scope of this Agreement, except with the Disclosing Party's written permission. Each Party agrees to protect the confidentiality of the Confidential Information of the other Party in the same manner that it protects the confidentiality of its own proprietary and confidential information of like kind (but in no event using less than reasonable care). Each Party may disclose Confidential Information to its directors, officers, employees, agents, advisors, Affiliates, independent contractors and consultants (collectively, "Representatives") on a "need to know" basis only, provided that such Representatives are bound by confidentiality obligations as least as a restrictive as those set forth in this Agreement. If the Receiving Party is compelled by law to disclose Confidential Information of the Disclosing Party, it shall

provide the Disclosing Party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party was to contest the disclosure.

3.2. End User Information. "End User Information" is data and material collected, received, processed or maintained by DeleteMe in connection with the Business Purpose. End User Information belongs to the Authorized User assigned to the Subscription from which the End User Information is provided. Each Authorized User is responsible for a) the accuracy of End User Information and b) obtaining any applicable authorizations required to provide the End User Information to DeleteMe. End User Information is subject to the disclosure, usage, access, transfer, processing, and retention protections and restrictions, including liability and warranty obligations, detailed in DeleteMe's Terms of Service and Privacy Policy.

3.3. Confidentiality. DeleteMe agrees that it will not (i) sell or share Confidential Information or End User Information that Buyer shares through the Services; (ii) retain, use or disclose Confidential Information or End User Information Buyer shares for any purpose other than the Business Purpose set out in the Agreement; or (iii) combine the End User Information DeleteMe receives from, or on behalf of Buyer with End User Information that DeleteMe receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless authorized by this Agreement or an applicable data protection law. DeleteMe agrees to (i) use or process End User Information only for the Business Purpose of performing the Services as described in this Agreement, unless required otherwise by a data protection law to which DeleteMe is subject; (ii) allow Buyer to take reasonable and appropriate steps to ensure that DeleteMe is using the End User information in a manner consistent with DeleteMe's obligations under this Agreement and data protection laws; (iii) notify Buyer of any inability of DeleteMe to comply with an applicable data protection law, including the California Consumer Privacy Act (CCPA) or the California Privacy Act (CPRA), within thirty (30) business days of DeleteMe making that determination; (iii) provide Buyer the right, upon notice, to take reasonable and appropriate steps to stop and remediate DeleteMe's unauthorized use of End User Information; (iv) provide Buyer with reasonable cooperation and assistance as Buyer may reasonably request to comply with Buyer's obligations under data protection laws, including but not limited to, consumer requests, risk assessments, and responding to applicable government authorities, and (v) allow Buyer to monitor DeleteMe's compliance with this Agreement through measures that include, but are not limited to, manual reviews, regular assessments, audits and technical testing, which shall not occur more than once every 12 months.

3.4. Subprocessor. A "Subprocessor" means any person (including any third party, but excluding an employee of DeleteMe) appointed by or on behalf of DeleteMe to process End User Information on behalf of Buyer in connection with the Agreement. DeleteMe will impose the same data protection duties and obligations applicable to DeleteMe on any Subprocessor utilized by DeleteMe to fulfill DeleteMe's obligations under this Agreement. DeleteMe shall remain solely responsible and liable to Buyer for any breach of this Agreement that is caused by an act, error or omission of its Subprocessors or other third party appointed by and acting under the authority of DeleteMe as if such acts or omissions were by DeleteMe.

3.5. Security Breach. A "Security Breach" means any confirmed act or omission that compromises the security, confidentiality, or integrity of End User Information or the physical, technical, administrative, or organizational safeguards put in place to protect it. DeleteMe shall notify Buyer without undue delay upon DeleteMe or any Subprocessor becoming aware of a Security Breach affecting End User Information, providing Buyer with sufficient information to allow Buyer to meet Buyer's reporting obligations under applicable data protection laws.

4. Term. This Agreement will remain in effect for twelve (12) months from its Effective Date ("Initial Term") and may be renewed for successive twelve (12) month periods by executing a written order("Renewal Term"). Buyer authorizes DeleteMe to charge Buyer's payment method on file or invoice Buyer for payment on the Effective Date of each Order and upon each renewal. Buyer may provide notice of nonrenewal to DeleteMe by contacting Buyer's Account Manager, or contacting DeleteMe at sales@joindeleteme.com,

+1-833-335-3836, or Abine Inc., 1 Marina Park Drive, Suite 1410, Boston, MA 02210. Buyer agrees to be charged now and upon each renewal until Buyer cancels. Buyer acknowledges its right to cancel.

4.1 Changes to Subscriptions After Renewal Notice Period. Buyer acknowledges and agrees that, after the deadline to provide notice of nonrenewal specified above, the Subscription structure (including but not limited to quantity of Subscriptions and scope of Services) will be deemed locked for the next Subscription Term. Any requested changes to Subscription structure or scope of Services after the nonrenewal deadline and prior to or after renewal may be accepted or rejected by DeleteMe in its sole discretion. If DeleteMe agrees to accept any requested changes, any adjustment in fees shall be made prospectively and not retroactively unless otherwise agreed in writing.

5. Termination. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, DeleteMe shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

6. Publicity. Buyer agrees that DeleteMe may use Buyer's name and logo for marketing and other promotional purposes, upon Buyer's advance written consent and to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

7. No Warranties. DELETEME WARRANTS THAT THE DELETEME SERVICES WILL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH DELETEME SERVICES WRITTEN MATERIALS ACCOMPANYING IT. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, FOR PURPOSES OF CLARIFICATION, ALL USE OF THE DELETEME SERVICES IS AT THE USER'S SOLE RISK AND THE DELETEME SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." DELETEME, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS MAKE NO EXPRESS WARRANTIES AND DISCLAIM ALL IMPLIED WARRANTIES REGARDING THE SERVICES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, TOGETHER WITH ANY AND ALL WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE IN TRADE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM DELETEME OR ELSEWHERE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT.

8. Limitation of Liability & Indemnity.
8.1 Exclusion of Damages. DELETEME, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO BUYER FOR ANY INDIRECT, INCIDENTAL, SPECIAL CONSEQUENTIAL, OR EXEMPLARY DAMAGES INCURRED BY BUYER OR USERS, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, INCLUDING, BUT NOT LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL, OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSS. THE FOREGOING LIMITATIONS ON DELETEME'S LIABILITY APPLY WHETHER OR NOT DELETEME HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING. NOTWITHSTANDING THE FOREGOING, NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS DELETEME'S LIABILITY FOR LOSSES THAT MAY NOT BE LAWFULLY EXCLUDED OR LIMITED BY APPLICABLE LAW. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM DELETEME'S GROSS NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

8.2 Liability Cap. THE TOTAL LIABILITY OF DELETEME ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL NOT EXCEED THE AMOUNT OF SUBSCRIPTION FEES PAID BY BUYER UNDER THE APPLICABLE ORDER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE LIABILITY.

8.3 Indemnification. DeleteMe ("Indemnifying Party") shall defend, indemnify, and hold harmless the Buyer, its officers, employees, and agents (collectively, "Indemnified Party") from and against any third-party claims, liabilities, damages, losses, and expenses, including reasonable attorney's fees, arising out of or relating to: (a) any gross negligence or willful misconduct of the Indemnifying Party; or (b) the Indemnifying Party's violation of applicable law. The indemnification obligations are conditioned upon prompt written notice of any claim and reasonable cooperation by the Indemnified Party in the defense of the claim. For the avoidance of doubt, this Section does not include intellectual property indemnification unless otherwise agreed in writing.

9. U.S. Government Users. The Services are "commercial items" as that term is defined at 48 C.F.R. 2.101; consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Services (including any licensed software) with only those rights that are set forth explicitly in the terms of use.

10. Notices. All notices, requests, consents, claims, demands, waivers, and other communications hereunder shall be in writing and shall be deemed to have been given: (a) when delivered by hand (with written confirmation of receipt); (b) when received by the addressee if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by email to a monitored email address if sent during normal business hours of the recipient, and on the next Business Day if sent after normal business hours of the recipient; or (d) on the third day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid.

11. Miscellaneous. The Services and any related technical data may not be exported, re-exported or used in any manner in violation of the laws, statutes, executive orders or regulations of the United States of America or of any country to which the same has been legally exported or re-exported. Each Party agrees to comply with all applicable United States and foreign export law, regulations, and license restrictions relating to the Services. The Parties agree that, irrespective of the place of performance of the Services, this Agreement will be governed by the Federal laws of the United States. The application of the UN Convention of International Sale of Goods to this Agreement is disclaimed in its entirety. Waivers and amendments of any provision of this Agreement shall be effective only if made by non-preprinted agreements indicating specifically what sections of this Agreement are affected, signed by both Parties and clearly understood by both Parties to be an amendment or waiver. The failure of either Party to enforce its rights under this Agreement at any time for any period shall not be construed as a waiver of such rights. If any provision of this Agreement is held invalid or unenforceable, the remainder of this Agreement will continue in full force and effect and the invalid or unenforceable provision shall be reformed to the extent necessary to make it valid and enforceable. Nothing contained herein will in any way constitute any association, partnership, or joint venture between the parties, nor does either Party have the power to bind the other Party or incur obligations on the other Party's behalf without the other Party's prior written consent.

The undersigned have executed this Business Subscription Purchase Agreement as of the Effective Date.

ABINE, INC. DBA DELETEME	**[COMPANY NAME]**
_____	_____
Rob Shavell, CEO Date	_____ Date

Privacy Policy

Effective Date: May 22, 2025

Executive Summary

At DeleteMe, your privacy is our priority. This Privacy Policy explains what personal information we collect, why we collect it, and how we use and protect it. Our goal is to be transparent, give you control, and uphold our commitment to removing your personal data from data broker sites. If you have any questions, we're here to help.

This Privacy Policy describes how Abine, Inc. dba DeleteMe and our corporate subsidiaries and affiliates (collectively, "DeleteMe", "we", "us", or "our") collects, uses and shares your personal information if you visit **joindeleteme.com** or our other websites or services that link to this Privacy Policy (collectively, the "Services"), contact us, receive our communications or attend our events. If you are looking for information on our use of cookies, please review our **Cookie Policy** below. We also provide important information for visitors located in **Europe and the United Kingdom** below.

Previous versions of our privacy policy:

- **05/19/2023**
- **08/21/2022**
- **11/22/2021**
- **12/31/2019**

Personal Information We Collect

Information you provide to us. Personal information you provide to us through the Services may includes:

- **Contact information**, such as your first and last name, email address, phone number, professional title and organization name.
- **Profile information**, such as your username and password and any account preferences for the Services.
- **Datasheet information**. When enrolling in the service, you will be asked to fill out a datasheet with personal data fields that you can choose to complete so that we can find instances of data brokers holding that data about you and have it deleted. The kinds of categories that you can provide and thus have us search against include first name, middle name, last name or surname/family name, date of birth, gender,

email addresses, phone numbers, street addresses, relatives' names, employers, political affiliation, and ethnicity ("Datasheet Data").

This Datasheet Data information is used to provide the DeleteMe service, specifically to search for listings containing your personal information on data broker websites and to have them removed. Providing this Datasheet Data information to us is entirely optional. The more information you provide, the more data points we can search against and the more listings we can potentially find and have deleted.

- **Feedback or correspondence**, such as information you provide when you contact us with questions, feedback, or otherwise correspond with us.
- **Usage information**, such as information about how you use the Services and interact with us, including information you provide when you use any interactive features of the Services.
- **Marketing information**, such as your preferences for receiving communications about our products, activities, and publications, and details about how you engage with our communications.
- **Other information** that we could collect is not specifically listed here but that we will use in accordance with this Privacy Policy or as otherwise disclosed at the time of collection.
- **Social media platform data.** Information we obtain from social media platforms. We may maintain pages for DeleteMe on social media platforms, such as Facebook, Twitter, and LinkedIn. When you visit or interact with our pages on those platforms, the platform provider's privacy policy will apply to your interactions and their collection, use, and processing of your personal information. You or the platforms may provide us with information through the platform, and we will treat such information in accordance with this Privacy Policy.
- **Information from other third parties.** Information we obtain from other third parties. We may receive personal information about you from third-party sources, such as marketing partners, publicly-available sources, and data providers.
- **Cookies and Other Information Collected by Automated Means.** We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and activity occurring on or through the Services. The information that may be collected automatically includes your computer or mobile device operating system type and version number, manufacturer and model; device identifier; browser type; screen resolution; IP address; the website you

visited before browsing to our website; general location information such as city, state or geographic area; and information about your use of and actions on the Services, such as pages or screens you viewed, how long you spent on a page or screen, navigation paths between pages or screens, information about your activity on a page or screen, access times, and length of access. Our service providers and business partners may collect this type of information over time and across third-party websites and mobile applications. See our **Cookie Policy** for more information.

How We Use Your Personal Information

We use your personal information for the following purposes and as otherwise described in this Privacy Policy or at the time of collection:

To operate the Services. We use your personal information to:

- **Provide, operate, and improve the Services** including using your Datasheet Data to search for listings containing your personal information on data broker websites and requesting that information be removed from those data broker websites;
- **Establish and maintain your user profile** on the Services;
- **Facilitate social features of the Services**, such as our blog;
- **Communicate with you about the Services**, including by sending you announcements, updates, security alerts, and support and administrative messages;
- **Understand your interests and personalize your experience** with the Services;
- **To send you marketing and promotional communications**, as permitted by law and with your consent where legally required. You can opt out of our marketing and promotional communications as described below;
- **For research and development purposes**, to analyze the use of our sevices in order to improve them and to develop new products/services;
- **To comply with the law** in instances where we have to share your data in order to comply with applicable laws, lawful requests, and legal processes, such as to respond to subpoenas or requests from government authorities;
- **For compliance, fraud prevention and safety** where we must use and/or disclose your personal data to law enforcement, government authorities and private parties as we believe is legally necessary or appropriate to (a) protect our, your, or others'

rights, privacy, safety, or property (including by making and defending legal claims); (b) enforce the terms and conditions that govern the Services; and (c) protect, investigate, and deter against fraudulent, harmful, unauthorized, unethical, or illegal activity;

- **To create anonymized data** from your personal information in order to analyze your data with a lower risk to you, the user;
- **provide support and maintenance** for the Services; and
- **respond to your requests**, questions and feedback.
- **To send you SMS messages**, if you opt in. No mobile opt-in data will be shared with third parties.

How We Share Your Personal Information

Datasheet Data Disclosures

Any Datasheet Data you enter on your datasheet may be disclosed by us to third parties such as data broker websites in the form of searches containing your personal information, to provide the Services. Such Datasheet Data disclosures are solely to request, on your behalf, that your personal information be removed from those data broker websites, and we do not share your Datasheet Data with third parties for any other reason.

General Data Disclosures

We share your personal information only as necessary to provide and improve our Services, comply with legal obligations, or fulfill other purposes described in this Privacy Policy. We do not sell your personal information. We limit disclosures to trusted partners under strict contractual terms and only for legitimate business purposes, as outlined below:

Affiliates. We may share your personal information with our corporate subsidiaries and any other individual, corporation, partnership, joint venture, limited liability entity, governmental authority, unincorporated organization, trust, association, or other entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, DeleteMe (“Affiliates”) for purposes consistent with this Privacy Policy.

Service providers. We may share your personal information with third-party companies and individuals that provide services on our behalf or help us operate the Services (such as customer support, hosting, analytics, email delivery, marketing, communications and database management services). These third parties may use your personal information only as authorized by their contracts with us.

Partners. We may sometimes share your personal information (excluding your Datasheet Data) with business partners or enable them to collect information directly via our Services. See our **Cookie Policy** for more information about third parties that collect information through our Services with cookies and similar technologies.

Third-party platforms and social media networks. If you have enabled features or functionality that connect the Services to a third-party platform or social media network (such as by connecting your account with a third party to the Services or sharing content via a third-party platform), we may disclose the personal information that you authorized us to share (excluding your Datasheet Data). We do not control the third party's use of your personal information.

Professional advisors. We may disclose your personal information to professional advisors, such as lawyers, bankers, auditors, and insurers, where necessary in the course of the professional services that they render to us.

For compliance, fraud prevention and safety. We may share your personal information for the compliance, fraud prevention and safety purposes described **above**.

Government Requests. Notwithstanding anything to the contrary in this policy, we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, or legal request or to protect the safety, property, or rights of DeleteMe or others. However, nothing in this policy is intended to limit any legal defenses or objections that you may have to a third party or government request to disclose your information.

Business transfers. In the event of a business transaction—such as a merger, acquisition, restructuring, or sale of assets—we may transfer your personal information as part of that transaction. If such a transaction occurs, we will provide notice to affected users where required by applicable data protection laws.

Any successor organization would be required to handle your personal data in accordance with this Privacy Policy or one with substantially similar protections. Importantly, DeleteMe does not sell your personal data as part of our business operations, and our commitment to privacy and data protection remains at the core of what we do.

Your Choices

In this section, we describe the rights and choices available to all users. Users who are located within Europe or the UK can find additional information about their specific data protection rights **below**.

Access or update your information. If you have registered for an account with us, you may review and update certain personal information, including Datasheet Data, in your account profile by logging into your account.

Opt out of marketing communications. You may opt out of marketing emails by following the unsubscribe instructions at the bottom of the email. You may continue to receive service-related and other non-marketing emails.

Cookies & browser web storage. For information on how to disable cookies and similar technologies used in the Services, see our **Cookie Policy**.

Do Not Track and Global Privacy Control. Some Internet browsers may be configured to send "Do Not Track" signals to the online services that you visit. We currently do not respond to "Do Not Track" or similar signals. To find out more about "Do Not Track," please visit **www.allaboutdnt.com**.

Choosing not to share your personal information. Where we are required by law to collect your personal information, or where we need your Datasheet Data to provide the Services to you, if you do not provide this information when requested (or you later ask to delete it), we may not be able to provide you with the Services. We will tell you what information you must provide to receive the Services by designating it as required at the time of collection or through other appropriate means. As described above, while you do not need to fill out your datasheet, we search for your personal data held by data brokers based on what you provide in the datasheet. The more information you provide in your datasheet, the more data points we can search against and the more listings we can potentially find and have deleted.

Third-party platforms or social media networks. If you choose to connect to the Services via a third-party platform or social media network, you may have the ability to limit the information that we may obtain from the third party at the time you connect your third-party account to the Services. Subsequently, you may be able to control your settings through the third-party platform. If you withdraw our ability to access certain information from a third-party platform or social media network, that choice will not apply to information that we have already received from that third party.

Other Sites, Mobile Applications, and Services

The Services may contain links to, or content or features from, other websites and online services operated by third parties. These links are not an endorsement of, or representation that we are affiliated with, any third party. In addition, our content may be included on web pages or in mobile applications or online services that are not associated with us. We do not control third-party websites, mobile applications, or online services, and we are not

responsible for their actions. Other websites and services follow different rules regarding the collection, use, and sharing of your personal information. We encourage you to read the privacy policies of the other websites and mobile applications and online services you use.

Artificial Intelligence Practices

DeleteMe may use artificial intelligence (AI) tools to support internal operations and improve service performance. However, we do not use AI tools to make automated decisions that significantly impact users. We prohibit the use of AI systems to process customer personal data unless such tools operate in secure, DeleteMe-controlled environments. Your personal data is never sent to untrusted third-party AI providers. DeleteMe recognizes that the use or disclosure of Government data for any purpose including, but not limited to, training artificial intelligence/machine learning models and systems, is prohibited without explicit written authorization from the ordering activity contracting officer. Government data means any information, (including metadata), document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by the Government, or a contractor on behalf of the Government, in the course of official Government business. For the avoidance of doubt, the contracting officer expressly consents to DeleteMe's use of end user personal information for the purpose of improving DeleteMe's service and offerings. For further details about our responsible use of AI, visit: **https://trustshare.joindeleteme.com**

Security Practices

We implement industry-recognized security best practices to protect your information. However, no security system is entirely impenetrable, and due to the inherent nature of the Internet, we cannot guarantee absolute protection against unauthorized access during transmission or while data is stored on our systems. To mitigate risks, we adhere to best practices such as enforcing encryption for all data in transit and at rest (TLS 1.2+ and AES-256), implementing robust access controls with multi-factor authentication (MFA), and continuously monitoring for threats through intrusion detection and endpoint security solutions. We also follow secure software development lifecycle (SDLC) principles, including regular security testing and vulnerability management. Additionally, we encourage you to take precautions, such as using strong, unique passwords and managing access to your logged-in devices. Our Governance, Risk and Compliance program transparently shares our comprehensive security controls addressing our security practices, and can be accessed at the following website: **https://trustshare.joindeleteme.com**

International Data Transfers

We are headquartered in the United States and have service providers in other countries, and so your personal information (excluding your Datasheet Data that is only stored in the United States) may be transferred outside of your state, province, or country to the United States or other locations where privacy laws may not be as protective as those in your state, province, or country. We will ensure that appropriate measures are in place for compliance with applicable data protection laws in relation to the transfer of your personal information to the United States. If you have any questions about where your data is stored, please email us at **support@joindeleteme.com**.

Your California Privacy Rights

Under California law, California residents are entitled to ask us for a notice identifying the categories of personal customer information that we share with certain third parties for marketing purposes, and providing contact information for such third parties.

If you are a California resident and would like a copy of this notice, please submit a written request to us via email at **support@joindeleteme.com**. You must put the statement "Your California Privacy Rights" in your request and include your name, street address, city, state, and ZIP code. We are not responsible for notices that are not labeled or sent properly, or do not have complete information.

The California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA) collectively referred to as the "CCPA/CPRA" provide certain rights to residents of California. If the CCPA/CPRA is applicable to you, you have the right to:

1. know the categories of personal information collected about you in the prior 12 months and its sources and business purpose;
2. know whether your personal information is sold or disclosed, and to whom, in prior 12 months;
3. opt out of the sale or sharing of your personal information;
4. access and then delete your personal information (subject to exceptions);
5. equal service and price (non-discrimination) if you exercise your privacy rights;
6. limit the use of your sensitive personal information; and
7. correct your personal information.

Contact us at **support@joindeleteme.com** to exercise your CCPA/CPRA rights.

Request for Erasure. For identity verification purposes, DeleteMe requires anyone submitting an erasure request to submit the subject's full name, email address, and home

address related to the subject's DeleteMe account or DeleteMe communications. DeleteMe will submit a verification email to the requestor who will be required to re-authenticate the request for erasure. DeleteMe relies upon this information to ensure the information on the correct individual is removed.

DeleteMe Subscribers Removal of Personal Information. Current members are able to log into their DeleteMe accounts to request personal data deletions on their user dashboards, which will also cancel their DeleteMe service subscriptions because, given the nature of the services we provide, we cannot provide the service without any personal data.

Do Not Sell My Information. We take your privacy seriously. We do not sell our members information. We are not a data broker.

If you are a California resident, you can request information regarding the disclosure, if any, of your personal information by DeleteMe to third parties for the third parties' direct marketing purposes. To make such a request, please send an email to **support@joindeleteme.com**, subject line: CCPA Request.

Your Nevada Rights

You may review and request changes to your information or opt-out of the sale of your personal information by emailing us at **support@joindeleteme.com**.

Notice to European & UK Users/Visitors

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

The information provided in this section applies only to individuals in the **European Economic Area** and the United Kingdom (collectively, "Europe").

Personal information. References to "personal information" in this Privacy Policy are equivalent to "personal data" governed by European data protection legislation.

Controller and Representative. DeleteMe is the controller of your personal information covered by this Privacy Policy for purposes of European data protection legislation.

Legal bases for processing. The legal bases of our processing of your personal information as described in this Privacy Policy will depend on the type of personal information and the specific context in which we process it. However, the legal bases we typically rely on are set out in the table below. We rely on our legitimate interests as our legal basis only where

those interests are not overridden by the impact on you (unless we have your consent or our processing is otherwise required or permitted by law). If you have questions about the legal basis of how we process your personal information, contact us at **support@joindeleteme.com**.

PROCESSING PURPOSE (CLICK LINK FOR DETAILS) DETAILS REGARDING EACH PROCESSING PURPOSE LISTED BELOW ARE PROVIDED IN THE SECTION ABOVE TITLED "HOW WE USE YOUR PERSONAL INFORMATION".	LEGAL BASIS
To operate the Services	Processing is necessary to perform the contract governing our provision of the Services or to take steps that you request prior to signing up for the Services. If we have not entered into a contract with you, we process your personal information based on our legitimate interest in providing the Services you access and request.
For research and development **To send you marketing communications** **For compliance, fraud prevention and safety** **To create anonymous data**	These activities constitute our legitimate interests.
To comply with law	Processing is necessary to comply with our legal obligations.
With your consent	Processing is based on your consent. Where we rely on your consent you have the right to

	withdraw it at any time in the manner indicated when you consent or in the Services.

Use for new purposes. We may use your personal information for reasons not described in this Privacy Policy where permitted by law and the reason is compatible with the purpose for which we collected it. If we need to use your personal information for an unrelated purpose, we will notify you and explain the applicable legal basis.

Sensitive personal information. We ask that you not provide us with any unnecessary sensitive personal information (e.g., social security number, government-issued identification, payment card information, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background or trade union membership) outside of what is required to provide the Services. All fields where sensitive data is requested in our product or service are optional for completion.

Retention

We retain personal information where we have an ongoing legitimate business need to do so (for example, to provide you with a service you have requested; to comply with applicable legal, tax or accounting requirements; to establish or defend legal claims; or for fraud prevention). When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

Data is stored in line with our internal retention policy. Identifying data provided by an active DeleteMe member will be retained for as long as the individual has a membership, plus 6 months. The 6 month buffer provides time for: any legal obligations, as well as a reasonable time-frame whereby the customer may reactivate their membership. Payment data will be stored for at least 7 years in line with the Generally Accepted Accounting Principles (GAAP) of the United States.

Your rights

European data protection laws give you certain rights regarding your personal information. If you are located within Europe, you may ask us to take the following actions in relation to your personal information that we hold:

- Access. Provide you with information about how we process your personal information and give you access to your personal information.
- Correct. Update or correct inaccuracies in your personal information.
- Delete. Delete your personal information.
- Transfer. Transfer a machine-readable copy of your personal information to you or a third party of your choice.
- Restrict. Restrict the processing of your personal information.
- Object. Object to our reliance on our legitimate interests as the basis of our processing of your personal information that impacts your rights.

Please contact our **EU Representative** to submit these requests. We may request specific information from you to help us confirm your identity and process your request. Applicable law may require or permit us to decline your request. If we decline your request, we will tell you why, subject to legal restrictions. If you would like to submit a complaint about our use of your personal information or our response to your requests regarding your personal information, you may contact our EU Representative or submit a complaint to the data protection regulator in your jurisdiction. **You can find your data protection regulator here**.

EU Representative

Our EU representative is our point of contact for EU data subjects and data protection supervisory authorities. To get in touch with our representative, please contact:

Postal Address: Pridatect, Pridatect, S.L., C/ del Marqués de Campo, nº 13, 46007, Valencia, Spain.

Phone number: +34 936 403 472

Email: **eurepresentation@pridatect.com**

Cross-Border Data Transfer

As a US-based organization, DeleteMe uses US-based providers to deliver the service. There is no functional international data transfer to processors or subprocessors and your data will remain in the US. However, you – as the data subject – should be aware that any data you provide is being sent directly to a US company that operates and provides our service in the US. Therefore, you are directly exporting your personal data to a third country. Please contact our **EU Representative** if you have any related questions.

Notification of changes and acceptance of policy

We keep our Privacy Policy under review and will place any updates on this webpage. By using DeleteMe, or any of our related services, you accept our collection and use of data by us as set out in this Privacy Policy attached hereto in order for us to fulfill obligations in the delivery of our services. Continued access or use of DeleteMe services will constitute your express acceptance of any non-material modifications to this Privacy Policy. If we are obliged to inform you of drastic changes, you will receive an email detailing these changes.

Children

The Services are not directed to, and we do not knowingly collect personal information from, anyone under the age of 16. If we learn that we have collected personal information of a child without the consent of the child's parent or guardian, we will delete it. DeleteMe does not provide services directly to anyone under the age of 18. We encourage parents or guardians with concerns to **contact us**.

Changes to this Privacy Policy

We may amend this Privacy Policy at any time by posting the amended version on the Services and indicating the effective date of the amended version. We may announce any material changes to this Privacy Policy through the Service and/or via email if we have your email address. You will have thirty (30) days after such announcement to object to the Privacy Policy changes. If we cannot come to an agreement about our Privacy Policy changes after a good faith effort by the parties, you may terminate the agreements between us and receive a pro-rata refund of fees. In all cases, your continued use of the Services after the posting of any modified Privacy Policy indicates your assent to the amended Privacy Policy.

Transparency and Government Requests

We believe in transparency regarding government requests for user data. As of **May 22, 2025**, Abine, Inc. (dba DeleteMe) has **never received** a National Security Letter, FISA order, or any other classified request for user information.

Should this statement ever be removed or updated, it would be an indication that we have received such a request that we are legally prohibited from disclosing. We will continue to update this statement regularly to maintain transparency with our users.

How to Contact Us

If you have any questions or comments about this Policy or DeleteMe's privacy practices, email us at **support@joindeleteme.com**. You may also write to us via postal mail at:

DeleteMe
Attn: Legal – Privacy
1 Marina Park Drive, Suite 1410
Boston, MA 02210

DeleteMe®

DELETEME'S DATA PROCESSING ADDENDUM

This DATA PROCESSING ADDENDUM ("DPA") between Abine, Inc. dba DeleteMe, (the "Provider") and _____, (the "Customer"), forms part of the Terms of Service or any other written agreement that governs Customer's use of the data broker opt-out solution provided by the Provider (the "Services") (collectively, the "Subscription Agreement"). This DPA becomes part of the Subscription Agreement upon execution by both parties and is incorporated in the Subscription Agreement by reference. This DPA is effective as of the same date as the Business Subscription Agreement.

The Provider provides the Services to the Customer under the Subscription Agreement that may require the Provider to process Personal Information provided by or collected for the Customer.

DPA TERMS

This Data Processing Addendum (the "DPA") sets out the additional terms, requirements, and conditions on which the Provider will obtain, handle, process, disclose, transfer, or store Personal Information when providing services under the Subscription Agreement.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. Definitions and Interpretation

1.1 The following definitions and rules of interpretation apply in this DPA.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with, the subject entity, where control is the direct or indirect ownership or control of at least a majority of the voting rights, or otherwise the power to direct the management and policies, of the entity. An entity is an Affiliate only so long as such control continues.

"Authorized Persons**"** means the persons or categories of persons that the Customer authorizes to give the Provider personal information processing instructions, as identified in Appendix A, if applicable.

"Business Purpose**"** means the services described in the Subscription Agreement or any other purpose specifically identified in Appendix A.

"CCPA/CPRA" means the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, and the regulations promulgated thereunder, as it/they may be amended from time to time.

"Contracted Processors" means Provider or a Subprocessor.

"Customer Personal Data" means any personal data processed by a Contracted Processor on behalf of Customer or any Customer Affiliate pursuant to or in connection with the Subscription Agreement.

"Data Subject**"** means an individual who is the subject of the Personal Information and to whom or about whom the Personal Information relates or identifies, directly or indirectly and (as applicable) (i) an identified or identifiable natural person who is in the EEA or whose rights are protected by the GDPR, the UK GDPR; or (ii) a "Consumer" as the term is defined in the CCPA/CPRA.

"EU Data Protection Legislation" means EU General Data Protection Regulation 2016/679 ("GDPR"), European Directive 2002/58/EC, the United Kingdom General Data Protection Regulation (UK

GDPR), the UK Data Protection Act of 2018, and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them.

“EEA” means European Economic Area.

"Personal Information**"** means any information the Provider processes for the Customer that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in the Provider's possession or control or that the Provider is likely to have access to, or (b) the relevant Privacy and Data Protection Requirements otherwise define as protected personal information including any information that identifies a Data Subject which information is subject to the GDPR, or the UK GDPR or, CCPA/CPRA, or other relevant Privacy and Data Protection Requirements.

"Processing, processes, or process**"** means any activity that involves the use of Personal Information or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Information to third parties.

"Privacy and Data Protection Requirements**"** means all applicable federal, and state, and foreign laws and regulations relating to the processing, protection, or privacy of the Personal Information, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Services Agreement. These include the GDPR, the UK GDPR, the CCPA/CPRA, and any other replacement laws or regulations as may be in force and applicable, from time to time.

“Restricted Transfer” means (a) a transfer of Customer Personal Data from Customer or Customer Affiliate to a Contracted Processor; or (b) an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Privacy and Data Protection Requirements (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Privacy and Data Protection Requirements) in the absence of the Standard Contractual Clauses.

"Security Breach" means the confirmed actual or reasonably suspected unauthorized access, use, disclosure, modification, destruction, or loss of Customer Personal Data, or any other event that compromises the confidentiality, integrity, or availability of Customer Personal Data.

"Standard Contractual Clauses (SCC)**"** means the European Commission's standard contractual clauses for the transfer of personal data from the European Union to third countries, as set out in the Annex to Commission Decision (EU) 2021/914, a completed copy of which comprises Appendix B, and the incorporated UK addendum to the standard contractual clauses for the transfer of personal data from the UK, a complete copy of which comprises Appendix C.

“Subprocessor” means any person (including any third party and any Provider Affiliate, but excluding an employee of Provider or any of its sub-contractors) appointed by or on behalf of Provider or any Provider Affiliate to Process Personal Data on behalf of any Customer in connection with the Subscription Agreement.

1.2 This DPA is subject to the terms of the Subscription Agreement and is incorporated into the Subscription Agreement. Interpretations and defined terms set forth in the Subscription Agreement apply to the interpretation of this DPA.

1.3 The Appendices form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Appendices.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Appendices, the provision in the body of this DPA will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Appendices, the provision contained in the Appendices will prevail;

(c) any of the provisions of this DPA and the provisions of the Subscription Agreement, the provisions of this DPA will prevail; and

(d) any of the provisions of this agreement and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

2. Personal Information Types and Processing Purposes

2.1 The Customer retains control of the Personal Information and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

2.2 Appendix A describes the general Personal Information categories and related types of Data Subjects the Provider may process to fulfill the Business Purposes of the Subscription Agreement.

3. Provider's Obligations

3.1 The Provider will only process, retain, use, or disclose the Personal Information to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. The Provider will not process, retain, use, or disclose the Personal Information for any other purpose or in a way that does not comply with this DPA or the Privacy and Data Protection Requirements. The Provider must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Privacy and Data Protection Requirements.

3.2 The Provider must promptly comply with any Customer request or instruction requiring the Provider to amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing.

3.3 The Provider will maintain the confidentiality of all Personal Information, will not sell it to anyone, and will not disclose it to third parties except with third-party companies and individuals that provide services on the Provider's behalf or help the Provider provide the Services (such as data brokers, customer support, hosting, analytics, email delivery, marketing, communications and database management services) or unless the Customer or this DPA specifically authorizes the disclosure, or as required by law. If a law requires the Provider to process or disclose Personal Information, the Provider must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of the Provider's processing and the information available to the Provider.

3.5 The Provider must promptly notify the Customer of any changes to Privacy and Data Protection Requirements that may adversely affect the Provider's performance of the Subscription Agreement.

3.6 The Customer acknowledges that the Provider is under no duty to investigate the completeness, accuracy, or sufficiency of any specific Customer instructions from Authorized Persons or the Personal Information other than as required under the Privacy and Data Protection Requirements.

4. Provider's Employees

4.1 The Provider will limit Personal Information access to:

(a) those employees who require Personal Information access to meet the Provider's obligations under this DPA and the Subscription Agreement; and

(b) the part or parts of the Personal Information that those employees strictly require for the performance of their duties.

4.2 The Provider will ensure that all employees:

(a) are informed of the Personal Information's confidential nature and use restrictions and are obliged to keep the Personal Information confidential;

(b) have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPA.

4.3 The Provider will take reasonable steps to ensure the reliability, integrity, and trustworthiness of, and conduct background checks consistent with applicable law on, all of the Provider's employees with access to the Personal Information.

5. Security

5.1 The Provider must at all times implement appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, unavailability, or damage.

(a) Provider’s Service Organization Controls 2 (“SOC 2”) audit report will demonstrate the trustworthiness of the Services, and that Provider has implemented essential data security controls. Upon request, Provider shall make available its most current SOC 2 audit report.

5.2 The Provider will immediately notify the Customer if it becomes aware of any advance in technology and methods of working, which indicate that the parties should adjust their security measures.

5.3 The Provider must take reasonable precautions to preserve the integrity of any Personal Information it processes and to prevent any corruption or loss of the Personal Information, including but not limited to establishing effective back-up and data restoration procedures.

6. Security Breaches and Personal Information Loss

6.1 The Provider shall notify Customer without undue delay upon Provider or any Subprocessor becoming aware of a Security Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer or any Customer Affiliate to meet any obligations to report or inform Data Subjects of the Security Breach under Privacy and Data Protection Requirements.

6.2 The Provider shall co-operate with Customer and any Customer Affiliate and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Security Breach.

7. Cross-Border Transfers of Personal Information

7.1 If the Privacy and Data Protection Requirements restrict cross-border Personal Information transfers, the Customer will only transfer that Personal Information to the Provider under the following conditions:

(a) the Provider, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, as identified in Appendix A, may legally receive that Personal Information, however the Provider must immediately inform the Customer of any change to that status;

(b) the Customer obtained valid Data Subject consent to the transfer under the Privacy and Data Protection Requirements; or

(c) the transfer otherwise complies with the Privacy and Data Protection Requirements for the reasons set forth in Appendix A.

7.2 If any Personal Information transfer between the Provider and the Customer requires execution of Standard Contractual Clauses in order to comply with the Privacy and Data Protection Requirements, the parties will complete all relevant details in, and execute, the Standard Contractual Clauses contained in Appendix B, and/or Appendix C and take all other actions required to legitimize the transfer, including, implementing any needed supplementary measures or supervisory authority consultations.

7.3 The Provider will not transfer any Personal Information to another country unless the transfer complies with the Privacy and Data Protection Requirements.

8. Subprocessing

8.1 Customer and any Customer Affiliate authorizes Provider and each Provider Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 8 to appoint) Subprocessors in accordance with this section 8 and any restrictions in the Subscription Agreement.

8.2 Provider and each Provider Affiliate may continue to use those Subprocessors already engaged by Provider or any Provider Affiliate as of the date of this DPA, subject to Provider and each Provider Affiliate in each case as soon as practicable meeting the obligations set out in section 8.4.

8.3 Provider shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within

ten (10) business days of receipt of that notice, Customer notifies Provider in writing of any objections (on reasonable grounds) to the proposed appointment neither Provider nor any Provider Affiliate shall appoint (nor disclose any Customer Personal Data to) the proposed Subprocessor except with the prior written consent of Customer.

8.4 With respect to each Subprocessor, Provider or the relevant Provider Affiliate shall:

(a) before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 8.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Subscription Agreement;

(b) ensure that the arrangement between on the one hand (a) Provider, or (b) the relevant Provider Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this DPA and meet the requirements of article 28(4) of the GDPR and all other Privacy and Data Protection Requirements;

(c) if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Provider, or (b) the relevant Provider Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Customer Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Customer or Customer Affiliate (and Customer shall procure that each Customer Affiliate party to any such Standard Contractual Clauses cooperates with their population and execution); and

(d) provide to Customer for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Customer may request from time to time.

8.5 Provider and each Provider Affiliate shall ensure that each Subprocessor performs the obligations under sections 3, 4, 5, 6, 7, and 9 as they apply to Processing of Customer Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of Provider.

9. Data Subject Rights and Data Protection Impact Assessment

9.1 Taking into account the nature of the Processing, Provider and each Provider Affiliate shall assist Customer and any Customer Affiliate by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the Customer or Customer Affiliates' obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Privacy and Data Protection Requirements.

9.2 Provider shall:

(a) promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any of the Privacy and Data Protection Requirements in respect of Customer's Personal Data; and

(b) ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or the relevant Customer Affiliate or as required by applicable Privacy and Data Protection Requirements to which the Contracted Processor is subject, in which case Provider shall to the extent permitted by Privacy and Data Protection

Requirements inform Customer of that legal requirement before the Contracted Processor responds to the request.

9.3 The Provider and each Provider Affiliate shall provide reasonable assistance to Customer and any Customer Affiliates with any data protection impact assessments, and prior consultations with data privacy authorities, which Customer reasonably considers to be required of any Customer or Customer Affiliates under Privacy and Data Protection Requirements, in each case solely in relation to the Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Term and Termination

10.1 This DPA will remain in full force and effect so long as:

(a) the Subscription Agreement remains in effect; or

(b) the Provider retains any Personal Information related to the Subscription Agreement in its possession or control (the "Term").

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Subscription Agreement in order to protect Personal Information will remain in full force and effect.

10.3 The Provider's failure to comply with the terms of this DPA is a material breach of the Subscription Agreement. In such event, the Customer may terminate any part of the Subscription Agreement authorizing the processing of Personal Information effective immediately upon written notice to the Provider without further liability or obligation.

10.4 If a change in any Privacy and Data Protection Requirement prevents either party from fulfilling all or part of its Subscription Agreement obligations, the parties will suspend the processing of Personal Information until that processing complies with the new requirements. If the parties are unable to bring the Personal Information processing into compliance with the Privacy and Data Protection Requirement, they may terminate the Subscription Agreement upon written notice to the other party.

11. Data Return and Destruction

11.1 On termination of the Subscription Agreement for any reason or expiration of its term, the Provider will securely destroy or, if directed in writing by the Customer, return and not retain, all or any Personal Information related to this agreement in its possession or control.

11.2 If any law, regulation, or government or regulatory body requires the Provider to retain any documents or materials that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. The Provider may only use this retained Personal Information for the required retention reason or audit purposes.

11.3 The Provider will certify in writing that it has destroyed the Personal Information after it completes the destruction.

12. Records

12.1 The Provider will keep detailed, accurate, and up-to-date records regarding any processing of Personal Information it carries out for the Customer, including but not limited to, the access, control,

and security of the Personal Information, approved subcontractors and affiliates, the processing purposes, and any other records required by the applicable Privacy and Data Protection Requirements (the "Records").

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this DPA.

12.3 The Customer and the Provider must review the information listed in the Appendices to this DPA once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 Upon the Customer's written request, the Provider will make any relevant audit reports available to the Customer for review. The Customer will treat such audit reports as the Provider's confidential information under this Agreement.

13.2 The Provider will promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of any applicable corrective actions.

14. Warranties

14.1 The Provider warrants and represents that:

(a) its employees, subcontractors, agents, and any other person or persons accessing Personal Information on its behalf are reliable and trustworthy and have received the required training on the Privacy and Data Protection Requirements relating to the Personal Information; and

(b) it and anyone operating on its behalf will process the Personal Information in compliance with both the terms of this DPA and all applicable Privacy and Data Protection Requirements and other laws, enactments, regulations, orders, standards, and other similar instruments; and

(c) it has no reason to believe that any Privacy and Data Protection Requirements prevent it from providing any of the Subscription Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Information and the accidental loss or destruction of, or damage to, Personal Information, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction, or damage; and

(ii) the nature of the Personal Information protected; and

(iii) comply with all applicable Privacy and Data Protection Requirement and its information and security policies, including the security measures required in 5.1.

14.2 The Customer warrants and represents that the Provider's expected use of the Personal Information for the Business Purpose and as specifically instructed by the Customer will comply with all Privacy and Data Protection Requirements.

15. Indemnification

15.1 The Provider agrees to indemnify, keep indemnified, and defend at its own expense the Customer against all costs, claims, damages, or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider or its employees, subcontractors, or agents to comply with any of its obligations under this DPA or applicable Privacy and Data Protection Requirements.

16. Notice

16.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to:

For the Customer: _____

For the Provider: legal@joindeleteme.com

16.2 16.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the date set forth above.

ABINE, INC. DBA DELETEME	**CUSTOMER:_____**
By _____	By _____
Name: Rob Shavell	Name:
Title: CEO	Title:

APPENDIX A

Data Processing Purposes and Details

Business Purposes:

Data broker listing removals.

Personal Information Categories:

Customer may submit Personal Data to the Services, the extent of which is determined by the Customer per the Service that is subscribed to. Customer can configure data fields during the implementation of the Service or as otherwise provided by the Service. The transferred Personal Data typically relates to the following categories of data: Name, email address, phone number, address, system access/usage/authorization data, company name, invoice data, and application-specific data that Authorized Users enter into the system.

Data Subject Types:

The Personal Data transferred hereunder relates to the following categories of Data Subjects: Authorized Users provided access to use the Services by Customer, employees, contractors, business partners or other individuals having Personal Data Processed by the Service.

Approved Subprocessors:

Amazon Web Services

Klaviyo

SendGrid

Snowflake

Abine India Private Limited

Authorized Persons:

Identify the Provider's legal basis for receiving Personal Information with cross-border transfer restrictions (select one):

	Located in an EEA Member State or in a country with a current determination of adequacy (list country):
	Binding Corporate Rules
X	Standard Contractual Clauses
	Other (describe in detail):

APPENDIX B

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
b. The Parties:
    i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
    ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

    have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
    i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
    iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
v. Clause 13;
vi. Clause 15.1(c), (d) and (e);
vii. Clause 16(e);
viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

i. where it has obtained the data subject's prior consent;
ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

a. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
b. of its identity and contact details;
    i. of the categories of personal data processed;
    ii. of the right to obtain a copy of these Clauses;
    iii. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
c. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
d. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
e. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

a. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
b. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
c. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
b. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
c. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
d. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
e. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
f. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
g. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless

the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

a. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
b. The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall

provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same

time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

a. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
b. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
c. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
d. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
b. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
c. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
d. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
e. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
f. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
g. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

a. The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
b. The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
c. The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
d. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

a. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for

the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

c. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

a. The Parties shall be able to demonstrate compliance with these Clauses.

b. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

a. The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
    i. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
b. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
c. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.
d. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

a. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
b. In particular, upon request by the data subject the data importer shall, free of charge :
    i. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
    ii. rectify inaccurate or incomplete data concerning the data subject;
    iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
c. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

d. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
    i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
    ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
e. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
f. The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
g. If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

   The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   ii. refer the dispute to the competent courts within the meaning of Clause 18.
d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.
c.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
    i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
    ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
    iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]
f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
   [For Module Three: The data exporter shall forward the notification to the controller.]

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
   [For Module Three: The data exporter shall make the assessment available to the controller.]

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    ii. the data importer is in substantial or persistent breach of these Clauses; or
    iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

    In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Spain

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
b. The Parties agree that those shall be the courts of Spain.
c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
d. The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller
Any dispute arising from these Clauses shall be resolved by the courts of Spain.

APPENDIX C

ANNEX I

A. **LIST OF PARTIES**

MODULE ONE: Transfer controller to controller: N/A

MODULE TWO: Transfer controller to processor: Customer to Abine, Inc. dba DeleteMe

MODULE THREE: Transfer processor to processor: Abine, Inc. dba DeleteMe to Hosting Provider

MODULE FOUR: Transfer processor to controller; N/A

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Entity Name: _____

Address: _____

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses: SaaS application platform to remove personal data from data brokers' websites.

Signature:_____ Dated: _____

Role: Controller

2. **Data importer(s):** [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

a. Name: Abine, Inc. dba DeleteMe

Address: 1 Marina Park Drive, Suite 1410, Boston, MA 02210

Contact person's name, position and contact details: Terressa DeHaven terressa.dehaven@joindeleteme.com; Reuben Moretz reuben.moretz@joindeleteme.com

Activities relevant to the data transferred under these Clauses: SaaS application platform to remove personal data from data brokers' websites

Signature:_____ Dated: _____

Role: Processor

B. **DESCRIPTION OF TRANSFER**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: The Personal Data transferred hereunder relates to the following categories of Data Subjects**:** Authorized Users provided access to use the Services by Customer, employees, contractors, business partners or other individuals having Personal Data Processed by the Service.

Categories of personal data transferred: Customer may submit Personal Data to the Services, the extent of which is determined by the Customer per the Service that is subscribed to. Customer can configure data fields during the implementation of the Service or as otherwise provided by the Service. The transferred Personal Data typically relates to the following categories of data: Name, email address, phone number, address, system access/usage/authorization data, company name, invoice data, and application-specific data that Authorized Users enter into the system.

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 (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: N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous

Nature of the processing: Abine, Inc. dba DeleteMe ("DeleteMe"), a provider of services which includes software applications and services geared towards removing personal data from data broker websites which DeleteMe may process upon the instruction of the data exporter in accordance with the terms of the Agreement.

Purpose(s) of the data transfer and further processing:

The Personal Data is subject to the following basic processing activities: Use of the Personal Data to setup, operate, monitor and provide the Service (including technical support); Provision of professional services; Communication with Authorized Users; Storage of Personal Data in designated data centers; Uploads of updates or upgrades to the Service; Back up of Personal Data; Processing of Personal Data, including transmission, retrieval, and access; Execution of instructions of Customer in accordance with the Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Duration of Contract Term

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: The transfers to sub processors follow the same processing activities and are subject to the same contract clauses as above

C. **COMPETENT SUPERVISORY AUTHORITY**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: For Data Exporters located in EU Member States the supervisory authority shall be EUROPEAN DATA PROTECTION SUPERVISOR

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) 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.

Measures of pseudonymisation and encryption of personal data

Pseudonymization: Pseudonymization is not applicable to data processed in the application(s).

Encryption: Personal data in application(s) is encrypted in transit and at rest. Personal data is encrypted for transit both to and from the data exporter and for any server-to-server communication necessary for the normal functioning of the application(s). The application(s) uses only private asymmetric keys and prohibits the use of master symmetric keys. Data at rest is encrypted and protected by access controls. Only authenticated users can read, modify, or delete data as specified by the permissions associated with their account.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Disaster recovery plans are in place for all application(s). For applications where data is stored, all employees of processor, by written policy, are prohibited from accessing a users' account without express written permission from the user or the data exporter.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Disaster recovery plans are in place for all application(s). Data backups are geo-replicated for applications that store data.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

During each phase of application(s) development, security measures are in place to identify and manage potential vulnerabilities throughout development and release. These include, but are not limited to:

OWASP Top 10 Vulnerabilities

Security and Privacy Risk Assessments

Threat Modeling

Static and Dynamic Code Analysis

Third-Party Penetration Testing

Measures for user identification and authorization

The following features exist to support the security of the accounts:

Privilege Levels

Automatic sign out

Failed Log-Ins Restrictions

Account De-Activation

Once accounts are established, processor offers two methods of user authentication: 1) Password-based authentication through the processors License Portal; and 2) Authentication through a third-party identity provider.

Measures for the protection of data during transmission

Data in all applications is encrypted in transit.. Data is encrypted for transit both to and from the data exporter and for any server-to-server communication necessary for the normal functioning of the application(s). The application(s) uses only private asymmetric keys and prohibits the use of master symmetric keys. Information at rest is encrypted and protected by access controls.

Measures for the protection of data during storage

Data in all applications is encrypted at rest utilizing database encryption methodologies provided by the hosting provider with no less than AES-256 encryption.

Measures for ensuring physical security of locations at which personal data are processed

DeleteMe does not process data onsite and uses sub-processors.

Please see Annex III.

Measures for ensuring events logging

Security logs capture the following events:

User, system, or process identifier that triggered the event

Description of event

Date and time of event

Authorization information associated with the event

Security logs, which are protected from modification and destruction, are maintained for at least 365 days.

Measures for ensuring system configuration, including default configuration Measures for internal IT and IT security governance and management

The processor maintains an information security management system (ISMS), including risk management, change control, incident management, corrective measures and management oversight.

Measures for ensuring data quality

Data profiling and control of incoming data

Data pipeline design to avoid duplicate data

Automated regression testing as part of change management

Measures for ensuring limited data retention

Please see the applicable section of processors application agreement.

Measures for ensuring accountability

All employees of processor are trained and must acknowledge processor's cybersecurity policies. Compliance with policy is monitored and retraining is provided as needed.

All engineering staff of processor are formally trained on processors Secure Development Lifecycle. Processor performs static and dynamic analysis of application code and requires manual review of source code for each application.

Measures for allowing data portability and ensuring erasure

Please see the applicable section of processors application agreement.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

Processor maintains agreements with all sub-processors identified in Annex III requiring technical and organizational measures no less than those maintained by processor. Agreements contain additional terms including, but not limited to, providing assistance to the controller, processor, and data exporter as may be necessary.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. **Name**: Amazon Web Services (AWS) Platform
   Address: 410 Terry Avenue North Seattle, WA 98109
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): The AWS Platform provides a series of modular cloud services including computing, data storage, data analytics and machine learning. alongside a set of management tools to underpin the operations and security of the DeleteMe infrastructure.
2. **Name**: Klaviyo, Inc.
   Address: 125 Summer Street Floor 7, Boston, MA
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): The Klaviyo platform allows DeleteMe to connect and communicate with customers via email and SMS.

3. **Name**: Sendgrid, Inc.
   Address: 1801 California Street, Denver, CO
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): The Sendgrid platform allows DeleteMe to connect and communicate with customers via email.
4. **Name**: Snowflake, Inc.
   Address: Suite 3A, 106 East Babcock Street, Bozeman, Montana
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): The Snowflake platform allows DeleteMe to perform data analytics
5. **Name**: Abine India Private Limited
   Address: 4th Floor, Pride Quadra, 30, Bellary Rd, Bengaluru, Karnataka 560024
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Abine India Private Limited allows DeleteMe to perform ongoing support services

APPENDIX D

UK ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Abine, Inc. Trading name (if different): DeleteMe Main address (if a company registered address): 1 Marina Park Drive, Suite 1410, Boston, MA 02210 Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Terressa DeHaven Job Title: Legal Counsel Contact details including email: terressa.dehaven@joindeleteme.com Reuben Moretz Job Title: Head of Security Contact details including email: reuben.moretz@joindeleteme.com

Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	X The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: June 2021 Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Table 3:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	X		General Authorisation	6-10 days	Yes
3						
4						

Table 3: Appendix Information
"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex I – A. List of Parties at Attachment 3 of the DPA.

Annex 1B: Description of Transfer: Data required to remove user information from Data Brokers' systems.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: The Annex II organizational measures are outlined in the Approved EU SCCs which this Addendum is appended to.

Annex III: List of Sub processors (Modules 2 and 3 only): The Annex III subprocessors are outlined in the Approved EU SCCs which this Addendum is appended to and include:
Amazon Web Services
Klaviyo
Sendgrid
Snowflake
Abine India Private Limited

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: X Importer X Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:
"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:
"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:
"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:
"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:
"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:
"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    c. its direct costs of performing its obligations under the Addendum; and/or
    d. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

APPENDIX E

CCPA/CPRA RESTRICTIONS

1. Restrictions on Use and Disclosure.

1.1. Restrictions. The restrictions in this Section 1 apply for purposes of all personal information provided by or on behalf of Customer under the Subscription Agreement that is personal information as defined in and subject to the CCPA/CPRA.

1.2. As between Customer and Abine, Inc. dba DeleteMe ("DeleteMe"), for purposes of the CCPA/CPRA, Customer is a "business" and DeleteMe is (if CCPA/CPRA applies) a "service provider" (each as defined in the CCPA).

1.3. DeleteMe shall not retain, use, or disclose personal information obtained in the course of providing the Services except:

1.3.1. To process or maintain personal information on behalf of or at the direction of Customer and in compliance with the Subscription Agreement;

1.3.2. To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA/CPRA;

1.3.3. For internal use by DeleteMe to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;

1.3.4. To detect data security incidents, or protect against fraudulent or illegal activity; or

1.3.5. For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(4).

1.4. DeleteMe will not: (i) "sell" such personal information to any third party (for these purposes, "sell" has the meaning ascribed to it in the CCPA); (ii) share or process the personal information for targeted and/or cross context behavioral advertising; (iii) combine personal information with any other data if and to the extent this would be inconsistent with the limitations on service providers under the CCPA/CPRA.

1.5. For clarity, the restrictions in this Section 1 include retention, use or disclosure of such personal information by DeleteMe outside of the direct business relationship between DeleteMe and Customer.

1.6. DeleteMe certifies that it understands the restrictions in this Section 1 and will comply with them.