directly

Directly, Inc. Privacy Policy Statement

Last Updated and Effective as of May 18, 2021.

Download the previous version of our Privacy Policy

This Privacy Policy Statement ("**Privacy Policy**") explains how Directly collects and handles data, including your personal data. It applies to all our Services, including this website. *Please carefully read this Privacy Policy and the applicable Terms of Service agreements for Answers and CVA before you provide any personal data to Directly*. If you have any questions regarding the Services or our privacy practices that are not answered in this Privacy Policy, please contact us via our secure data request web form or at privacy@directly.com.

Table of Contents

1. Introduction

1.1. Directly Services. Directly.com and the related platform, software and services (collectively the "**Services**") are operated by Directly, Inc. ("**Directly**," "we," "our," "us" dba "Directly Software, Inc."). Directly provides the Services to deliver better customer service for our corporate enterprise customers ("**Customer(s)**"). The Services are comprised of two primary offerings: 1) "**Answers**," which uses the Answers technology platform and product experts ("**Expert(s)**") to provide best in class support to each Customer's end users ("**Customer End User(s)**"); and 2) "**Crowdsource Virtual Agent**" or "**CVA**," which uses the CVA technology platform to enable each Customer to deploy, continuously train and manage a virtual agent ("**VA**") through the digital customer care channels ("**Channels**") using specialist contributors ("**Specialists**").

Experts and Specialists hereinafter are referred to collectively in this Privacy Policy as "**Expert User(s).**" Expert Users can earn rewards for answering or classifying questions submitted by Customer End Users, either through personalized or automated responses (collectively "**Services Content**").

1.2. Purpose & Scope. This Privacy Policy describes how we collect, use and share different types of data, including personal data and the choices you have with respect to your personal data. By **"Personal Data**," we mean any type of information that identifies, or reasonably could be used to identify, you as an individual, as part of a household or associated with a device. Certain legal jurisdictions, for example, the European Economic Area countries "**EEA**," or the State of California, apply different definitions of personal data or similar terms. Where applicable, we will use that specific definition of personal data or similar applicable term. We refer to data that falls outside any applicable legal definition of personal data, such as publicly available, de-identified or anonymous data, as "**Other Data**." Personal Data and Other Data are referred to collectively as "**Data**." All capitalized terms not defined in this Privacy Policy are defined in the Answers Terms or CVA Terms, and your use of the Services is subject to the applicable Terms. By accessing directly.com or submitting Personal Data through the Services, you consent to the processing of your Personal Data in accordance with this Privacy Policy. If you do not agree with our Privacy Policy or respective Terms, do not access or use directly.com, the Services or any other aspect of Directly's business offerings, and in such case, you should (a) take the necessary steps to remove cookies from your computer after leaving our website and/or Services (see Section 2.3 below), and (b) discontinue any future access or use.

1.3. Minors. Our Services (including directly.com) are intended for adults and not for minors: Anyone under the age of 18 is not permitted to access or use the Services, except with Directly's prior written permission. You also must not permit any person under the age of 18 to access our Services. We do not intentionally gather personal data from minors under applicable legal age requirements. If a minor submits Personal Data to Directly and we learn that the Personal Data is of a child under the applicable age requirement, we will attempt to delete the Personal Data as soon as possible. If you believe that we may have any Personal Data of a child under the applicable age requirement, please contact Directly at legal@directly.com.

1.4. Scope of Application. The Privacy Policy applies to your access to and use of the Services, either as a visitor to directly.com or as an Expert User. This Privacy Policy does not apply in the following circumstances:

- First, the Privacy Policy does not apply to our Customers or our Customer's authorized personnel, whose license and access to the Services is governed by a separate legal agreement with Directly (each a "**Customer Agreement**") and, in certain cases, supplemental terms.
- Second, the Privacy Policy does not apply to Customer End Users who post customer service questions through independent websites, helpdesk systems and customer service channels managed by each Customer.

- Third, the Privacy Policy does not apply to any third-party websites or other digital properties, applications, services, products or software ("**Third-Party Services**") even if they link to or from or framed within directly.com or the Services, or any other third-party products, services or businesses such as our Customers. Accordingly, in each of these circumstances you should reference and review carefully the privacy policies and practices of those independent third parties.

2. Data Collected

2.1. Expert Users and Registration for a Directly Account. We collect Personal Data in different ways depending on the circumstances of your use of our Services and the choices you make about the Personal Data you submit to us. You can visit directly.com and certain subdomains without registering, but to become an authorized Expert User eligible to submit Services Content, you will need to create an account with Directly ("**Directly Account**") and submit the following types of Personal Data: legal name, email address and/or mobile phone number, a personal headshot photo, physical mailing address, legal residence information and regional location of access, birthdate, verification phone number and government identification ("**Expert Registration Information**"). We also automatically collect Data such as device information and internet protocol address ("**IP Address**"). As an Expert User, you must also select your username, sometimes referred to on our platform as your "alter ego." Please select your username carefully consistent with our Terms and your privacy preferences. Please read our current guidelines on the Expert User Hub as there are rules and privacy consequences for your username selection. Generally, we recommend that Expert Users do not use their full legal name, which could be used to identify them, or use a fanciful, misleading or inappropriate username. Expert Users also have the option to create user profiles describing why they should be considered Expert Users, as well as their top skills and language abilities. We use elements of the Expert User Registration Information to verify your identity, combat fraud and abuse and keep our Services, Expert Users, Customers and partners secure. By registering for a Directly account, you authorize us and/or our Third-Party Providers (as described below) to verify Expert User Registration Information, including your identity and background. As described in our Terms, Directly or Customers may impose additional terms and duties for your eligibility ("**Supplemental Terms**"). You will be given an opportunity to review and consent to such Supplemental Terms. For example, where a Customer or applicable data protection or other law requires special expert certification measures or other protocols, and subject to your consent, Expert Users may be asked to provide additional Personal Data relating to background, location of access or legal residence.

2.2. Log and Usage Information. We also collect other types of Data, which may be construed as Personal Data in certain jurisdictions and under certain contexts, including the following: usage information such as how you have used our Services, IP address and other technical data such as browser type, unique device identifiers and information, language preference, referring site and the date and time of access, operating system and mobile network information; approximate location data (from IP address); information regarding interactions with

our Services, such as votes on Services Content, feedback, comments, poll and survey responses and other information you may provide us.

2.3. Cookies. Please refer to Directly's Cookie Policy, which is incorporated in this Privacy Policy, for detailed information about the use of cookies and other tracking technologies on our website.

2.4. Data Collected by Third Parties. We also may process Data, including Personal Data, from certain third-party providers (each a "**Third-Party Provider**") who collect Data from you to verify, update or supplement the Data you provide, or we collect automatically. We use Third-Party Providers for functionalities and information needed to deliver the Services. For example, if you access our Services from the independent services of Third-Party Providers in connection such as the Apple App Store, Google Play, Salesforce App Store or another third-party app platform, you are subject to the privacy policies of the respective provider. Our Services and associated technology also enable one or more Third-Party Provider services (e.g., Google Analytics) to collect certain types of Data (such as device identifiers) so we can analyze how our Services are used. We may also link or integrate with certain Third-Party Providers, such as Jumio or ThreatMetrix, who collect personal data subject to separate terms and privacy policies for identity verification and fraud protection. Please remember that all Data collected by Third-Party Providers are governed by the respective provider's terms of service, privacy and other policies.

3. Use and Retention

3.1. Use. We and our Third-Party Providers use Data, including Personal Data to: (i) provide our Services; (ii) promote, analyze and improve our Services; (iii) comply with applicable law and enforce our Terms, and (iv) detect and prevent fraud, harmful or abusive conduct, or other injury to Expert Users, Customers, Directly or third parties. Some examples of how we may use Personal Data include:

● Creating your Directly Account;
● Identifying you on our system, and verifying your actual identity and Registration Information, to ensure the security and integrity of our Services and enable you to send or respond to certain routed Tasks;
● Responding to your inquiries to administer and improve our Services;
● Informing the applicable Customer of your relevant activity on the Services;
● Providing technical support and respond to inquiries by Expert Users and Customers;
● Soliciting input and feedback to improve and customize your Expert User experience;
● Informing you about new features, services and programs on the Services;
● Customizing your use of the Services and content or other material that we may send to you from time to time;
● Conducting aggregate analysis and business intelligence to enable us to better operate, protect, make informed decisions and improve and report on the performance of our Services and business performance;

● For audits, legal and regulatory purposes or compliance with industry and other standards;
● Preventing or taking action against conduct or content that is, or may be, in breach of our Terms, Privacy Policy, contractual or applicable law, including combating fraud and abuse; and
● For any other purpose, provided we disclose this to you at the relevant time, and where required, obtain consent to the proposed use of your Personal Data.

3.2. Retention. Where Directly is processing and using your Personal Data, we will store your Personal Data only for as long as required to fulfil the purposes set out herein and permitted to do so by applicable law. For example, where Directly is required by law to retain your Personal Data longer, or where your Personal Data is required for Directly to assert its legal rights or protect our Services, Directly, or third-party rights, we will retain your Personal Data until the end of the relevant retention period or until there is no longer a necessity. Please note that we have a variety of obligations to retain Personal Data you provide to us, including to ensure that rewards and associated payments can be appropriately processed and to protect our Services, Directly and third-party rights, consistent with applicable law and our legal obligations. Accordingly, even if you close your Directly Account, we may retain certain data to protect these rights and interests or meet these obligations.

4. Sharing and Disclosure

4.1. General. Directly does not sell or rent your Personal Data. We share Personal Data collected by Directly with Third-Party Providers only in defined circumstances, including: (i) with your consent; (ii) to an authorized Third-Party Provider who meets required privacy, security and data protection standards; or (iii) when we have a good faith belief it is required or permitted by law, such as pursuant to a subpoena or other legal process, or to enforce our Terms or legal rights.

4.2. Third-Party Providers. We share data with certain Third-Party Providers who help us provide the Services. For example, certain Third-Party Providers help us with such activities as web hosting, data analysis, fraud and integrity protection. Currently, we use Amazon for hardware, software, networking and storage services which are necessary to operate our website and Services. We also reserve the right to share Personal Data with Third-Party Providers, such as merchants (e.g., PayPal), application providers (e.g., Lessonly), and identity verification providers (e.g. Jumio and ThreatMetrix) as necessary to process payments, verify and qualify Expert Users and provide Services. Except as otherwise stated in this Privacy Policy, such Third-Party Providers are prohibited from using Personal Data other than to provide the services specified under written contract by Directly and for no other purposes. Subject to the foregoing, you expressly consent to the sharing of your Personal Data and Other Data with these Third-Party Providers for these limited purposes.

4.3. Third-Party Acquirer. If we merge with another company causing your Personal Data and Other Data to become subject to a materially different privacy policy, we will notify you before the transfer. You can opt out of any new policy by deleting your account during the notice period.

4.4. Expert Users. We disclose certain limited content of each request for Answers (e.g., non-personally identifiable usernames or first names of Expert Users). We also share Other Data with Expert Users about their responses to Answers and the generation of Services Content.

4.5. Customers and Customer End Users. We disclose the content of the responses (including the first name of the Expert User who responded) to the Customer who generated the request (and to any subsequent Customer End User that pose similar requests). When an Expert User responds to requests from Customer End Users, certain limited and filtered Data contained in the response, such as a username, the text of the response and other Personal Data (such as an Expert User's personal headshot or picture) will be accessible to Customers and Customer End Users. You understand and agree to the sharing of such Data.

4.6. Usage Data. Directly may use or disclose (except as expressly provided herein) the personal data of Expert Users, except where prohibited by applicable law or otherwise required by legal duty. Notwithstanding the foregoing and for the avoidance of doubt, Directly may use and disclose data about usage of the Services that does not identify or reasonably could be anticipated to be used to identify any individual user of the Services or otherwise constitute Personal Data ("**Usage Data**"). We share Usage Data about our website and Services with our business partners. We reserve the right to use and disclose Usage Data for any purpose and to any third parties subject to the terms herein.

4.7. Future Affiliates. Although we currently do not have a parent company, any subsidiaries, joint ventures or other companies under a common control (collectively, "**Affiliates**"), we may in the future. We may share some or all of your Personal Data with these Affiliates, in which case we will require our Affiliates to honor this Privacy Policy. If another company acquires our company or our assets, including pursuant to a bankruptcy or similar proceeding, that company will possess the Personal Data collected and stored by us and will assume the rights and obligations regarding your Personal Data as described in this Privacy Policy.

4.8. Legal Disclosures. We reserve the right to disclose your Other Data and Personal Data as required by law in connection with any legal investigation, when we believe that disclosure is necessary to protect our rights (or those of other Users or third parties) and/or to comply with a judicial proceeding, or valid court order, warrant, subpoena or legal process served on us.

4.9. Communications. We will send you service-related announcements when it is necessary or beneficial to do so. For instance, if our Services are temporarily suspended for maintenance, we might send you an email or other communications. We also may send you notifications on your mobile device and you may disable these notifications in the settings of your device. Based upon the Personal Data you provide us, we will send you a welcome email to verify your username and password. We will also communicate with you in response to your inquiries to provide the services you request, manage your Directly Account, solicit your feedback or update you on new policies. We will communicate with you by email or mobile phone in accordance with your indicated preferences. Please refer to Choices and Rights below.

5. Choices and Rights

5.1. Opt Out Choices. You have choices and access rights regarding our use and disclosure of your Personal Data. If you no longer want to receive marketing-related emails from us going forward, you may opt out via the unsubscribe link included in such emails. If you wish to access, amend or delete Personal Data we hold about you, or if you have any objection to the processing of any Personal Data that we hold about you, please complete our secure data request web form and submit it to us as instructed on the form. If you ask us to delete your account, we will do so within a reasonable period of time, but we may need to retain certain Personal Data in order to satisfy our legal obligations or where we have a legitimate reason for doing so. If your Personal Data changes, or if you no longer desire our Services, you may update or deactivate your Directly Account by making the change in your account page or by completing a secure data request web form. We may be required to keep your Data and not delete your Data (or to keep your information for a certain time, in which case we will comply with your deletion request only after we have fulfilled such requirements). When we delete any Data, it will be deleted from the active database, but may remain in our archives. After deactivation of your Directly Account and deletion of Data from the active database, we may continue to use and disclose your Personal Data in accordance with this Privacy Policy. If you decide that you do not want us to use your Data in the manner described in the Privacy Policy, you may not use the Services. If you have already registered an account, you can cancel your account or correct or delete your Data by completing a secure data request web form.

5.2. Access Rights. Individuals located in certain countries, such as the European Union or EEA, have certain statutory rights in relation to their Personal Data. Please read Section 7.5 below carefully so you understand all of your rights and how to exercise all of your rights.

6. Security. The security and protection of your Personal Data is important to us. We follow generally accepted industry standards to protect the Data submitted to us, both during transmission and once we receive such Data. No method of transmission over the Internet, or method of electronic storage, is 100% secure however. Therefore, while we strive to use commercially acceptable means to protect your Data, we cannot guarantee its absolute security. You use our Website and Services at your own risk, and you are responsible for taking reasonable measures to secure your account (like using a strong password). We urge you to take steps to keep your Personal Data safe (including your account password) and log out of your account after use. If your Directly Account is hacked, this may lead to unauthorized access, so be careful to keep your account data secure. We strongly recommend our Expert Users to use two factor authentication ("**2FA**") options. If you have any questions about 2FA options, contact security@directly.com.

7. Important Information for European Users

7.1. Data Export and Processing. Our Services are accessible globally. We store and process Personal Data on servers located in the United States, and we may transfer Personal Data (as

defined under applicable law) to countries outside of your country of residence, which may have data protection laws that are different from the laws of the country where you reside. We will take measures to ensure that any such transfers comply with applicable data protection laws and that your Personal Data remains protected to the standards described in this Privacy Policy. By using our Services, you consent to the transfer, storage and processing of your Personal Data in the United States in accordance with this Privacy Policy and applicable law.

7.2. Safeguards for Exports from EEA. If you are located in the EEA or Switzerland, we comply with applicable laws requiring adequate levels of data protection for the transfer of Personal Data. You agree that Directly may transfer your Personal Data to countries other than the one in which you live.

7.3. Legal Basis for Processing. If you are an individual residing in the EEA, we collect and process information about you only where we have legal bases for doing so under applicable EU laws. The legal bases depend on the specifics of the Services you use and how you use those Services. This means we collect and use your information only where:

- We need it to provide you with or operate the Services, including to provide customer support using Expert Users, personalize features, fulfill the contract you have with Directly (or Directly has with each Customer or third party), or protect the integrity and security of the Services;
- It satisfies a legitimate interest (which is not overridden by your data protection interests), such as for anti-fraud protection or to protect our legal rights and interests;
- You give us consent to do so for a specific purpose; or
- We need to process your data to comply with a legal obligation.

If you have consented to our use of your Personal Data for a specific purpose, you have the right to change your mind at any time, but this will not affect any processing that has already taken place. Where we are using your Personal Data because we or a third party have a legitimate interest to do so, you have the right to object to that use though, in some cases, this may mean no longer using the Services or associated services.

7.4. Identifying Data Controller and Data Processor and Different GDPR Roles. Data protection laws in certain jurisdictions differentiates between the “controller” and “processor” of data. It is important to note that Directly acts as both as a Data Controller and as a Data Processor within the scope of the GDPR (as described below): (a) As a Data Controller, Directly is responsible for safeguarding the Personal Data of our Users and visitors to directly.com; and (b) As a Data Processor, Directly is responsible for processing personal data in accordance with our Customer contracts and applicable law and safeguarding the data of Customer End Users. Directly’s Customers generally serve as the controller of its Customer End Users’ personal data. In this context, Directly serves as the processor of such personal data under instructions from each controller. Each Customer is also responsible for making sure that their respective Customer end user’s privacy rights are protected, including responding to data subject requests. Directly will respond to such data subject requests from Customers and Customer End Users as a Data Processor; this means with respect to Personal Data of Customer End Users we must respond as a matter of law and contract through our Customer. On the other hand, with respect

to Expert Users, Directly serves as the controller of Expert User Personal Data and will directly respond to data subject request rights from Expert Users.

7.5. Access Rights. Individuals located in certain countries, including the EEA or European Economic Area, have certain statutory rights in relation to their personal data. Subject to any exemptions provided by law, such individuals may have the right to request access to their Personal Data, as well as to seek to update, delete or correct this information. They also have a right to restrict or object to processing and to data portability, where applicable. We may be legally required or permitted to deny or part of your request and, if we do deny your request, we will endeavor to explain the reasons underlying our decision.

7.6. Data Protection Authority and Representative. Subject to applicable law, you may also have the right to (i) restrict Directly's use of certain data elements that constitute your Personal Data; and (ii) lodge a complaint with your local data protection authority or the Irish Data Protection Commissioner, which is Directly's lead supervisory authority in the European Union. If you are a resident of the European Economic Area and believe we maintain your Personal Data within the scope of the General Data Protection Regulation ("**GDPR**"), you may direct questions or complaints to our European GDPR representative. To find the data protection authority in your country, please refer to this contact list. Our GDPR Data Protection Representative is DataRep and can be contacted by sending an email to consultancy@datarep.com quoting "Directly, Inc." in the subject line.

8. California Users

Do Not Track Signals. As there is no accepted standard on how to respond to "**Do Not Track Signals**," we respond to such signals.

California Consumer Privacy Act. Notice for California Consumers. The California Consumer Privacy Act of 2018 ("**CCPA**") created specific privacy rights for California consumers. We share the same information about our practices with everyone, but use this notice to make disclosures required by the CCPA. This notice includes the following parts:

- **Transparency:** We are transparent about how your personal information is collected, used, shared and sold.
- **Control:** We put you in control of your personal information, including accessing and deleting your personal information.
- **Benefits to You:** We use your personal information to benefit you and to make your experiences better.
- **Transparency:** What Personal Information We Collect. You have the right to know what kinds of personal information Directly is collecting and our business purposes for that collection. We make this information available to consumers in the "Data Collected" Section 2 of this Privacy Policy.

How We Use Your Personal Information. You have the right to know how personal information is obtained, how it is used and our business purposes for that use. We make this information available to consumers in the "Use and Retention" Section 3 of this Privacy Policy.

How We Share Your Personal Information. You have the right to know if your personal information is shared with any third parties. We may share personal information to select Service Providers, as defined by the CCPA, who perform services specified by written contract. In addition, we may share personal information with third parties for other notified purposes as permitted by the CCPA. We make this information available to consumers in the "Sharing and Disclosure" Section 4 of this Privacy Policy.

We Do Not Sell Your Personal Information. You have the right to know whether your personal information is being sold. Your personal information is sold when it is shared with a third party for monetary or other valuable consideration for a purpose that is not a "business purpose" as set forth in the CCPA. Directly does not sell your personal information.

Control: Right to Know, Right to Receive, Right to Delete. You have the right to:

- Know what specific pieces of personal information Directly has collected and retained about you over the previous 12 months.
- Receive a copy of your personal information.
- Delete your personal information.

Directly aims to make it easy for you to exercise your rights by using our secure data request web form.

Right to "Opt Out" of "Sale." *Directly does not sell your personal information, so we do not offer an opt out.*

Benefits to You/Financial Incentives. The CCPA allows businesses to offer consumers financial incentives for sharing personal information. For example, a business can offer a rewards program or provide a premium service to consumers as compensation for their personal information. Where Directly offers these programs, your participation is optional. If you choose to participate, your participation will be subject to any applicable terms, and you may withdraw at any time.

Non-Discrimination. The CCPA prohibits businesses from discriminating against you for exercising your rights under the law. Such discrimination may include denying a good or service, providing a different level or quality of service or charging different prices. The CCPA permits businesses to provide differing levels or quality or different prices where the business can demonstrate that the difference is reasonably related to the value to the business of the consumer's personal information.

9. Changes. We may periodically update this Privacy Policy. If we make any substantial changes, we may notify you by sending you an email to the last email address you provided to us (if any) and/or by prominently posting notice of the changes on the website and via Services, so it is visible when you visit and/or log on to the website or Services for the first time after the change is posted. Your continued use of the website or the Services after the changes have been posted shall constitute your acceptance of the changes. If you do not agree to the updated Privacy Policy, you must cease your access and use of the websites and Services.

10. Contact Us. How do I contact Directly about questions or issues about my privacy? Any questions about this Privacy Policy or our practices with respect to your Data can be submitted via our secure data request web form.

11. Data Privacy FAQs

How do I request information about the data you process, request deletion, make a data request or ask a question?

If you wish to delete Personal Data you believe we hold about you, have another data rights request, or have a privacy or data protection related question, please use our secure data request web form and submit it to us as instructed. This form allows us to securely verify your identity so we can protect your privacy and fulfill your request in a timely manner.

How does Directly and its Services operate? As detailed in our Terms, Directly has entered into separate agreements with each Customer to govern the delivery, access and use of the Services including instructions for the processing of the personal data of their respective Customer End Users. Each Customer licenses Directly technology and configures their help desks to enable its Customer End Users to post Tasks to the Services for routing to Expert Users. It is important to note that Directly acts as both as a Data Controller and as a Data Processor within the realm of GDPR compliance: As a Data Controller, Directly is responsible for safeguarding the data of our Expert Users as they interact directly with our marketplace platform and our visitors to directly.com. As a Data Processor, Directly is responsible for safeguarding the data of our Customers Users as it flows through our marketplace platform.

Who is my Data Controller? If you are a visitor to directly.com or an Expert User of the Services, your Data Controller is Directly, Inc. If you are a Customer End User (i.e., an individual that posted a support request via a Customer's website or digital property), then the Data Controller of your personal data is your respective Customer and you should direct all questions about your Personal Data to that Customer.

What does Directly collect and do with my Personal Data? Directly will process your Personal Data as set out in this Privacy Policy. The Data we collect depends on how you use our website and Services. Sometimes, we receive Data directly from you, such as when you create a Directly Account to register as an Expert User, complete a form or send us an email. Other times, we collect Data by recording interactions with our website or Services. The

collection and use of Data from a variety of sources is essential to our ability to provide the Services, and to help keep it trustworthy and secure. Further information about our use of your Data and Personal Data can be found in Section 2.

Duration of processing of Personal Data. Where Directly is processing and using your Personal Data as permitted by law or under your consent, we will store your Personal Data (i) only for as long as is required to fulfill the purposes set out below; (ii) until you object to Directly's use of your Personal Data (where Directly has a legitimate interest in using your Personal Data); or (iii) until you withdraw your consent (where you consented to Directly using your Personal Data). However, where Directly is required by mandatory law to retain your Personal Data longer or where your Personal Data is required for Directly to assert or defend against legal claims, we will retain your Personal Data until the end of the relevant retention period or until the claims in question have been settled. See Section 3.2, "Retention," for details.

Why am I required to provide Personal Data? As a general principle, your granting of any consent and your provision of any Personal Data hereunder is entirely voluntary; there are generally no detrimental effects on you if you choose not to consent or to provide Personal Data. However, there are circumstances in which we cannot take action without certain Personal Data, for example, because this Personal Data is required to process your registration or provide you with access to our Services. In these cases, we cannot provide you with what you request without the relevant Personal Data.

Where will my Personal Data be processed? Directly is based and operates out of the United States. As a consequence, whenever Directly is using or otherwise processing your Personal Data for the purposes set out in this Privacy Policy, we may transfer your Personal Data to countries outside of the EEA, such as the United States, where such countries in which a statutory level of data protection applies that is not comparable to the level of data protection within the EEA. See Section 7, "European Users," above.

How do I determine which company is the "controller" of my personal information? Privacy and data protection law in certain jurisdictions differentiates between the "controller" and "processor" of data. Each Customer is the controller of its Customer End User's Personal Data, and in this context Directly serves as the processor of such personal data under instructions from each controller. Each Customer is also responsible for making sure that their respective customers or end user's privacy rights are protected, including responding to data subject requests. Directly will respond to such data subject requests from Customer End Users as a processor which means that it will contact and follow the advice of the controller Customer with respect to such requests. With respect to Personal Data of Expert Users, Directly serves as the controller of such data and will respond to data subject request rights. Please refer to Section 5, "Choices and Rights," above, for additional information on your rights. Expert Users can request information about the Personal Data Directly stores about you, and the correction or deletion of such Personal Data. Please note, however, that we can delete your Personal Data only if there is no statutory obligation or prevailing right of Directly to retain your Personal Data. If you request that Directly delete your Personal Data, you will not be able to continue to use the

Services that requires Directly's use of your Personal Data. See Section 5, "Choices and Rights," above. If you believe that Directly is not processing your Personal Data in accordance with the requirements set out herein or applicable EEA data protection laws, you can at any time lodge a complaint with the data protection authority of the EEA country in which you live or our GDPR Data Protection Representative. See Section 11 for details.

12. Appendix A to Privacy Policy: EU-U.S. and Swiss-U.S. Privacy Shield Policy.

Directly, Inc. ("**Directly**," "we," "our" or "us" dba "Directly Software, Inc.") has subscribed to the EU U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, "**Privacy Shield**"). Notwithstanding the current invalidation of the Privacy Shield by the European Court of Justice, Directly adheres to the Privacy Shield Principles including the Supplemental Principles (collectively, the "**Privacy Shield Principles**") for Personal Data received from entities in the European Economic Area (the "**EEA**") and Switzerland. This Privacy Shield Policy ("**Privacy Shield Policy**") describes our privacy practices for Personal Data received from the EEA or Switzerland in reliance on the Privacy Shield. This Privacy Shield Policy uses terms which are defined in our Privacy Policy. If there is any conflict between the terms in this Privacy Shield Policy and the Privacy Shield Principles as concerns the Personal Data received under the Privacy Shield, the Privacy Shield Principles shall govern to the extent of the conflict. To learn more about the Privacy Shield program visit www.privacyshield.gov, and to view our certification, please visit www.privacyshield.gov/list.

Privacy Shield Principles

1. Notice and Choice. Our Privacy Policy describes how we use Personal Data we receive from different sources. This Privacy Shield Policy describes how we process Personal Data covered by the Privacy Shield. If you are a Customer, Directly may act as an agent for you in relation to the Personal Data that you provide or make available to Directly. Directly usually does not have a relationship with any users or customers of our Customers, and each Customer is responsible for ensuring that their users are provided with appropriate notice and choice with respect to their Personal Data.

2. Data Integrity and Purpose Limitation. We only collect Personal Data that is relevant to providing our website and associated Services. We process Personal Data in a way that is compatible with us providing the Services to you, or in other ways, for which we will provide you with notification. We take reasonable steps to ensure that the Personal Data received under the Privacy Shield is needed for Directly to provide its Services, and to ensure data is accurate, complete and current.

3. Accountability for Onward Transfers. Directly may disclose Personal Data to trusted third parties as indicated in the Privacy Policy. Directly requires that its agents and service providers that have access to Personal Data within the scope of this Privacy Shield Policy provide the same level of protection as required by the Privacy Shield Principles. We ensure that our agents process Personal Data received under the Privacy Shield in a manner consistent with our

obligations under the Privacy Shield Principles, unless we prove that we are not responsible for the event giving rise to the damage. We may need to disclose Personal Data in response to lawful requests by public authorities for law enforcement or national security reasons, when such action is necessary to comply with a judicial proceeding or court order, or when otherwise required by law.

4. Data Security. We use reasonable and appropriate physical, electronic and administrative safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information.

5. Access to Personal Data. Our Privacy Policy explains how you may access and/or submit requests to review, correct, update, suppress or delete Personal Data. You can ask to review and correct Personal Data that we maintain about you by completing and submitting a secure data request web form. We may limit or deny access to Personal Data where providing such access is unreasonably burdensome, expensive under the circumstances or as otherwise permitted by the Privacy Shield Principles. When Directly acts on behalf of its Customers, Directly will assist Users in responding to individuals exercising their rights under the Privacy Shield Principles. **If you are a Customer End User, please contact the Customer directly with your request to access or limit the use or disclosure of your Personal Data.** If you contact us with the name of the Customer to which you provided your Personal Data, we will refer your request to that Customer and support them in responding to your access request.

6. Recourse, Enforcement and Dispute Resolution. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the Privacy Shield Principles. In compliance with the Privacy Shield Principles, Directly, Inc. commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Directly, Inc. using our secure data request web form here. Directly has further committed to refer unresolved Privacy Shield complaints to JAMS, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please visit JAMS Privacy Shield Dispute Resolution webpage for more information to file a complaint. The services of JAMS are provided at no cost to you.

7. Contact Information. If you have any questions regarding this Privacy Shield Policy, please contact us by submitting a secure data request web form.

8. Changes to this Privacy Shield Policy. This Privacy Shield Policy may be changed from time to time, consistent with the requirements of the Privacy Shield and in accordance with the process described in the Privacy Policy. You can determine when this Privacy Shield Policy was last revised by referring to the “Last Updated and Effective as of” date at the top of this page.

13. Addendum B to Privacy Policy: Expert User Data Protection Addendum

This Directly Data Processing Addendum (the "**DPA**") supplements, and is incorporated into, the Terms of Service (the "**Terms**") between Directly and you as an Expert User. The parties agree as follows:

1. Purpose and Scope.

1.1 Except as modified below, the Terms shall remain in full force and effect; if there is any conflict between this DPA and the Terms or any other agreement between the parties, the provisions of this DPA shall take precedence.

1.2 The European Union General Data Protection Regulation 2016/679 ("**GDPR**") requires all Expert Users to contractually undertake certain data protection commitments with respect to Personal Data (as described below) they may Process on Directly's behalf. To ensure compliance with the GDPR, Expert Users must agree to the terms of this DPA.

2. Definitions. All capitalized terms used but not defined in this DPA shall have the meaning given to them in the Terms.

2.1 "Confidential Information" means the definition ascribed in the Terms (see Terms, Section 7, Confidential Information).

2.2 "Data Protection Laws" means (a) any applicable law with respect to any Personal Data to which Directly is subject and (b) European Data Protection Laws.

2.3 "Data Subject Request" means a data subject's request to exercise that person's rights under Data Protection Laws in respect of that person's Personal Data, including, without limitation, the right to access, correct, amend, transfer, obtain a copy of, object to the Processing of, restrict the Processing of or delete such Personal Data.

2.4 "European Data Protection Laws" means the GDPR, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), any national laws or regulations implementing the foregoing Directives, any applicable legislation of European Union Member States passed to implement the foregoing and any other applicable data protection, privacy or data security laws or regulations in the European Economic Area, United Kingdom, Switzerland or any other applicable European jurisdiction, in each case, as they may be amended, replaced or supplemented from time to time.

2.5 "Expert User(s)" means a natural person who is a party to this DPA.

2.6 “Personal Data” means any information about an identified or identifiable natural person and any other “personal data” governed by applicable Data Protection Laws that Expert User processes in connection with the Expert User’s performance of the Services.

2.7 “Privacy Shield” means the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks established respectively by the European Commission and the United States Department of Commerce and the Swiss Administration and the United States Department of Commerce.

2.8 “Process” means any operation or set of operations which is performed on Restricted Information (as described below) or sets of Restricted Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.9 “Restricted Information” refers collectively to “Confidential Information” and “Personal Data” of any source and includes any information Processed by Expert User in connection with the Expert User’s performance of the Services.

2.10 “Security Incident” means a reasonably suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

2.11 “Services” means Expert’s authorized participation, activity and content on and through the platform Directly provides to its customers, including but not limited to, responses relating to tasks and questions about specific products and services for which the Expert is approved.

3. Your Data Protection Duties. You acknowledge and agree to the following:

3.1 You will Process Personal Data only in accordance with the Terms, Data Protection Laws and Directly’s written instructions communicated by Directly to you from time to time in writing.

3.2 Without limiting the generality of sub-section 3.1, you agree as follows:

3.2.1 You will keep all Restricted Information in strictest confidence and will not copy, use, store, disclose or otherwise Process any Restricted Information except to perform the Services;

3.2.2 You will take appropriate technical and organizational measures (including but not limited to the Expert Standards (which are incorporated herein and may be updated by Directly from time to time)) to ensure the confidentiality, integrity and availability of any computers or other systems that you use to perform the Services and protect against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Restricted Information transmitted, stored or otherwise Processed;

3.2.3 You will only subcontract, delegate or engage any other individual or entity to assist with performance of the Services with the prior written approval of Directly, and pursuant to the completion of a prior data protection and security audit, the implementation of additional data protection and security safeguards and other such measures as Directly reasonably determines is necessary under applicable law.

3.2.4 You will only subcontract, delegate or engage any other individual or entity to assist with performance of the Services with the prior written approval of Directly, and pursuant to the completion of a prior data protection and security audit, the implementation of additional data protection and security safeguards and other such measures as Directly reasonably determines is necessary under applicable law.

3.2.5 You will make available to Directly all information necessary to demonstrate compliance with the obligations set forth in this DPA and the Data Protection Laws and to allow Directly to conduct audits, including inspections, of your compliance with the obligations set forth in this DPA;

3.2.6 If instructed by Directly, you agree to promptly notify Directly and cooperate to provide the circumstances underlying any receipt or access of Personal Data and to confirm you have promptly and permanently deleted any such Personal Data in your possession, together with any existing copies, unless directed otherwise;

3.2.7 If you receive any request, demand or inquiry regarding Personal Data ("**Personal Data Request**") other than from Directly, including, without limitation, any Data Subject Request or other request received from a regulator or other governmental body, you agree to NOT respond to any such Personal Data Request except in accordance with Directly's written instructions or as otherwise required by the Data Protection Laws;

3.2.8 You will promptly and without undue delay cooperate, assist and take such action as Directly may reasonably request to allow Directly to fulfil its obligations to Customers and their Data Subjects or under Data Protection Laws in respect of such a Personal Data Request, including, without limitation, meeting any deadlines imposed by such obligations; you will notify Directly without undue delay and in no event later than 48 hours upon your becoming aware of a Security Incident, and provide Directly with sufficient information to allow it to meet any legal or contractual obligations to report the Security Incident;

3.2.9 You will cooperate with Directly and its authorized agents and representatives to take such reasonable steps as are directed by Directly to assist in the investigation, mitigation and remediation of any Security Incident;

3.2.10 You will provide reasonable assistance to Directly and its Customers with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Directly or its Customer reasonably considers to be required by the Data Protection Laws;

3.2.11 You will immediately inform Directly, in writing, if in your opinion, an instruction violates Data Protection Laws;

3.2.12 You agree to comply with the Privacy Shield principles set forth at www.privacyshield.gov and incorporated into our Privacy Policy and to take such actions and sign such documents (such as "**Standard Contractual Clauses**") as Directly may request to ensure that a valid cross-border data transfer mechanism recognized by European Data Protection Laws covers the Processing of Personal Data contemplated by this DPA if required by European Data Protection Laws.

4. General Terms.

4.1 The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Terms with respect to any disputes or claims however arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

4.2 This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in Terms, or if different, the laws required to govern under European Data Protection Laws.

4.3 Directly may amend this DPA from time to time as is reasonably necessary to comply with Data Protection Laws, and such amendments shall become binding upon giving Expert notice of such changes.