



**Liberty Common School**

1725 Sharp Point Dr. Fort Collins, CO 80525

**Liberty Common High School**

2745 Minnesota Dr. Fort Collins, CO 80525

**EXHIBIT A**

**CONFIDENTIALITY, PRIVACY, AND SECURITY ADDENDUM**

This Confidentiality Addendum (“Addendum”) is hereby incorporated into any Agreement between Liberty Common School (LCS) and \_\_\_\_\_ (Contractor). Attached after the Addendum is the referenced Agreement. This Addendum is part of the Contract between LCS and the Contractor.

**RECITALS**

- A. LCS wishes to disclose certain information to Contractor pursuant to the work being performed by Contractor, some of which may constitute Student Personally Identifiable Information (PII) (defined below).
- B. LCS and Contractor intend to protect the privacy and provide for the security of Student PII (PII) disclosed to Contractor pursuant to this Contract. Contractor shall adhere to 22-16-101 *et. al.*, C.R.S.; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99.

The parties agree as follows:

A. Definitions

- 1. "Aggregate Data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.

2. "Destroy" refers to data destruction, and means to remove Student PII from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with governing law and current industry standards, so that the Student PII is permanently irretrievable in the Contractor's and Subcontractor's normal course of business.
3. "Incident" means an accidental or deliberate activity that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources. Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a LCS system or Student PII regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a LCS system for the processing or storage of data; (iv) a material breach of the Contract that involves the misuse or unauthorized release of Student PII; or (v) changes to LCS system hardware, firmware, or software characteristics without LCS's knowledge, instruction, or consent.
4. "School Service" means an internet website, online service, online application, or mobile application that is designed and marketed primarily for use in a preschool, elementary school, or secondary school; is used at the direction of teachers or other employees of LCS; and collects, maintains, or uses Student PII. School Service does not include an internet website, online service, online application, or mobile application that is designed and marketed for use by individuals or entities generally, even if it is also marketed to a United States preschool, elementary school, or secondary school.
5. "School Service Contract Provider (Contractor)" means an entity, other than a public education entity or an institution of higher education that enters into a formal, negotiated contract with LCS to provide a School Service.
6. "Student PII" means information that, alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by a public education entity, either directly or through a School Service, or by a School Service Contract Provider. PII also includes other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
7. "Subcontractor" means any third party engaged by Contractor to aid in performance of Contractor's obligations. LCS understands that Contractor will rely on one or more subcontractors to perform services under this Agreement. Contractor agrees that all subcontractors, and any successor entities, will be subject to state and federal laws and to the terms of the Agreement, and any data disclosed to subcontractors shall be revealed to LCS upon request.

8. "Targeted Advertising" means selecting and sending advertisements to a student based on information obtained or inferred over time from the student's online behavior, use of applications, or PII. Targeted Advertising does not include advertising to a student at an online location based on the student's current visit to that location or in response to the student's request for information or feedback and is without the collection and retention of a student's online activities over time. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.
9. "Data" means all Student PII and other non-public information. Data may not be used for any purposes other than the specific purposes outlined in this Agreement.

#### B. General Provisions

1. LCS reserves all right, title, and interest, including all intellectual property and proprietary rights, in and to system data, PII, and all related data and content.
2. Contractor shall comply with all laws and regulations concerning confidentiality of PII.
3. Contractor shall immediately forward to LCS's principal representative any request or demand from a third party for PII in the possession of Contractor.
4. Upon request of LCS, Contractor shall submit its data processing facilities for an audit of the measures referred to in this Addendum by LCS or by a LCS approved delegate.
5. Contractor shall send LCS a written notice, which includes a clear explanation of the proposed changes prior to making a material change to Contractor's privacy policies. Contractor shall require LCS's informed consent before any new privacy policies are implemented.

#### C. Subcontractors

1. Contractor shall not use a Subcontractor or disclose PII to a Subcontractor unless and until the Contractor contractually requires the Subcontractor to comply with C.R.S. §§22-16-108 through 22-16-110 and the requirements of this Addendum.
2. If Contractor discovers that Subcontractor or any subsequent subcontractor has committed a material breach of the contract between Contractor and Subcontractor that involves the misuse or unauthorized release of PII, Contractor acknowledges that LCS may terminate the contract with Contractor.
3. Upon discovering the misuse or unauthorized release of PII held by a Subcontractor or any subsequent Subcontractor, Contractor shall notify LCS within one calendar day, regardless of whether the misuse or unauthorized release by the Subcontractor is a result of a material breach of the terms of the Contract or results in an Incident.
4. No later than thirty (30) days after the signing of this Contract, upon request of LCS, Contractor will provide LCS information detailing the purpose and the scope of the

contract between the Contractor and all Subcontractors and the types and uses of PII that Subcontractor(s) holds under the Contract between the Contractor and Subcontractor(s).

5. Contractor shall not maintain or forward PII to or from any other facility or location except for backup and disaster recovery purposes. Any backup or disaster recovery contractor shall be considered a Subcontractor that must comply with the Subcontractor requirements in this Addendum.

#### D. End of Agreement

1. Should Contractor not comply with the requirements of this Addendum and that non-compliance results in the misuse or unauthorized release of PII by the Contractor, LCS may terminate the Contract immediately as provided under this Contract and in accordance with C.R.S. Section 22-16-107 (2)(a).
2. Upon request by LCS made before or within thirty (30) calendar days after termination of the Contract, Contractor shall make available to LCS a complete and secure (i.e. encrypted and appropriately authenticated) download file of all data, including, but not limited to, all PII, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in its native format.
3. In compliance with the prescriptions of C.R.S. 22-16-110 (3), following the termination of this Contract, Contractor shall, within thirty (30) calendar days, Destroy all PII and data collected, generated, or inferred as a result of this Contract. The Contractor shall notify LCS of the date upon which all PII is Destroyed.
4. LCS retains the right to use the established operational services to access and retrieve PII stored on Contractor's infrastructure at its sole discretion.

#### E. Use

1. In compliance with C.R.S. 22-16-109 (1)(a), the Contractor shall not use or share PII beyond the purposes set forth as follows:
  - a. To only carry out the Contractor's responsibilities listed in Exhibit A, Statement of Work.
  - b. [Vendor to insert any services involving PII and the purposes for using PII].
2. In the event the Contract requires Contractor to store, process or transfer PII, Contractor shall store, process, and transfer PII only in or to facilities located within the United States.
3. During the term of this Contract, if LCS requests the destruction of a student's PII collected, generated or inferred as a result of this Contract, the Contractor shall Destroy the information within five calendar days after the date of the request unless:

- a. The Contractor obtains the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian to retain the student's PII; or
  - b. The student has transferred to another public education entity and the receiving public education entity has requested that the Contractor retain the student's PII.
4. If Contractor seeks to share or publicly release PII without complying with the requirements of this Addendum for Subcontractors, Contractor must de-identify or aggregate the PII prior to providing that information to a third party or releasing the data publicly. For data that is de-identified or aggregate, the following requirements apply:
- a. PII that must be aggregated or de-identified shall include not only direct identifiers, such as names, student IDs or social security numbers, but also any other sensitive and non-sensitive information that, alone or combined with other information that is linked or linkable to a specific individual, would allow identification.
  - b. Simple removal of direct identifiers from the data to be released shall not constitute adequate de-identification.
  - c. Contractor shall de-identify data to remove cumulative re-identification risks.
  - d. Contractor shall remove all PII that in conjunction with previous data releases and other reasonably available information, including publicly available directory information and de-identified data releases from education records and other sources would allow for identification of a particular student.
  - e. Contractor shall have specific steps and methods used to de-identify or aggregate information to protect the confidentiality of the individuals. Contractor shall, at the request of LCS, provide LCS with a document that lists the steps and methods the Contractor shall use to de-identify the information.
  - f. Any aggregate or de-identified data that is not properly de-identified or aggregated and is transferred to a third party without the controls of this Addendum for subcontractors or publicly released will be considered an Incident, misuse of PII, or unauthorized disclosure of PII.

#### F. Incident

1. If Contractor becomes aware of an Incident, misuse of PII, or unauthorized disclosure involving any PII, it shall notify LCS within one (1) calendar day and cooperate with LCS regarding recovery, remediation, and the necessity to involve law enforcement, if any.
2. Unless Contractor can establish that Contractor or any of its Subcontractors is not the cause or source of the Incident, Contractor shall be responsible for the cost of notifying each person whose personal information may have been compromised by the Incident.

3. Contractor shall determine the cause of an Incident and produce a remediation plan to reduce the risk of incurring a similar type of breach in the future. Contractor shall present its analysis and remediation plan to LCS within ten (10) calendar days of notifying LCS of an Incident. LCS reserves the right to adjust this plan, in its sole discretion. If Contractor cannot produce its analysis and plan within the allotted time, LCS, in its sole discretion, may perform such analysis and produce a remediation plan, and Contractor shall reimburse LCS for the reasonable costs thereof.
4. Disclosure of PII by Contractor or any Subcontractor for any reason may be cause for legal action by third parties against Contractor, LCS, or their respective agents. Contractor shall indemnify, save, and hold harmless LCS, its employees, and agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred as a result of any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees pursuant to this Addendum. Notwithstanding any other provision of this Contract, Contractor shall be liable to LCS for all direct, consequential, and incidental damages arising from an Incident caused by Contractor or its Subcontractors.
5. In the event of an Incident, Contractor shall provide LCS or its designated representatives with access seven (7) days a week, twenty-four (24) hours a day, for the purpose of evaluating, mitigating, or resolving the Incident.

#### G. Disallowed Activities

A Contractor that uses, creates, or acquires PII shall not knowingly engage in any of the following activities:

1. Contractor shall not collect, use or share PII for any purpose not specifically authorized by the Contract. Contractor may use PII for a purpose not strictly authorized by the Contract only with the written consent of LCS and with the written consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.
2. Contractor shall not use PII in a manner or disclose PII to any third party that is materially inconsistent with the Contractor's privacy policy, except as stated in subsection 3, below, of this Section G.
3. Contractor may use PII in a manner that is inconsistent with Contractor's privacy policy without violating the terms of this Contract provided that the use does not involve selling or using PII for Targeted Advertising or creating a personal profile of the student, and the use is for one or more of the following purposes:
  - a. To ensure legal or regulatory compliance or to take precautions against liability.
  - b. To respond or to participate in the judicial process.
  - c. To protect the safety of users or others on Contractor's website, online service, online application, or mobile application.

d. To investigate a matter related to public safety.

If Contractor uses or discloses PII in accordance with Section G.3., Contractor shall notify LCS within two (2) calendar days of the use or disclosure of the PII.

4. Contractor shall not sell PII, except that this prohibition does not apply to the purchase, merger, or other type of acquisition of the Contractor, or any assets of the Contractor, by another entity, so long as the successor entity continues to be subject to the provisions of this Contract.
5. Contractor shall not use or share PII with any party for the purposes of Targeted Advertising to students.
6. Contractor shall not use PII to create a personal profile of a student other than for supporting the purposes authorized by LCS or with the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.

#### H. Data Security

1. Contractor shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of PII. At a minimum, the information security program shall include the requirements listed in this Section H – Data Security.
2. Contractor shall provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this Contract. Contractor shall take full responsibility for the security of all PII in its possession, and shall hold LCS harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof. Contractor shall provide for the security of such PII, in a form acceptable to LCS, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, network firewalls, intrusion detection (host and network), data security logging and monitoring systems, and audits.
3. Contractor shall provide LCS or its designated representatives with access, subject to Contractor's reasonable access security requirements, for the purpose of inspecting and monitoring access and use of PII, maintaining LCS systems, and evaluating physical and logical security control effectiveness.
4. Contractor shall perform, in a form reasonably acceptable to LCS, current background checks on all of its respective employees and agents performing services or having access to PII provided under this Contract. The background checks must include, but are not limited to the following areas: County, State, National and Federal Criminal Records and a Sex Offender Registry Search. A background check performed within thirty (30) calendar days prior to the date such employee or agent begins performance or obtains access to PII shall be deemed to be current.

5. Contractor shall have strong access controls in place.
6. Workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended.
7. Contractor shall protect all PII with a complex password. Contractor shall ensure passwords are confidential and prohibit the sharing of passwords. Passwords must not be written down or stored in an unsecure location. Contractor shall periodically change passwords and shall ensure passwords are not reused. Contractor shall have password locks for laptops and mobile devices.
8. Contractor shall disable and/or immediately delete unused and terminated user accounts. Contractor shall periodically assess account inactivity for potential stale accounts.
9. Contractor shall not share PII on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.
10. Contractor shall implement annual intrusion penetration/vulnerability testing.
11. Contractor will encrypt PII in transit and PII at rest on central computing systems. Contractor shall also encrypt any backup, backup media, removable media, tape, or other copies. In addition, Contractor shall fully encrypt disks and storage for all laptops and mobile devices.
12. Contractor shall provide annual, mandatory security awareness and PII handling training for all of its employees/independent contractors handling PII pursuant to this Contract.
13. Contractor shall install and maintain on computers accessing or processing PII appropriate endpoint security anti-virus and anti-malware software. Contractor shall ensure all Contractor's data processing systems, servers, laptops, PCs, and mobile devices are regularly scanned and have all security patches applied in a timely manner.
14. Contractor shall use a secure method such as Secure File Transfer Protocol (SFTP) or comparable method to transmit PII. Contractor shall never send PII via email or transport PII on removable media.
15. Contractor shall have physical security in buildings housing PII, along with controlled physical access to buildings and/or data centers.
16. Contractor's devices used to copy or scan hard copies of PII must have encrypted storage. Contractor shall scrub storage devices when equipment is retired. Hard copies containing PII are discouraged and must be physically secured, not left unattended, and physically Destroyed.
17. Contractor shall protect PII stored in cloud-based systems in the same manner as local PII. Use of free cloud based services is prohibited. Contractor shall use secondary



encryption to protect PII in cloud storage. Cloud environments, when employed by Contractor, must be fully documented by Contractor and open to LCS inspection and verification. Access to Contractor's cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

#### I. Transparency Requirements

1. Contractor shall facilitate access to and correction of any factually inaccurate student PII in response to a request from a local education provider or from LCS.
2. Contractor acknowledges that LCS will post this Contract to LCS's website.
3. Contractor shall provide transparency to parents, school districts and the public about its collection and use of PII including posting the following information on its public website:
  - a. Contact information for an individual within Contractor's organization that can provide information on or answer questions related to the use of PII by Contractor.
  - b. An explanation of how the PII will be shared with Subcontractors or disclosed to any third party or successor entities.
  - c. The types of PII that are collected, generated, or used by the Contractor. This information must include all PII that is collected regardless of whether it is initially collected or ultimately held individually or in the aggregate.
  - d. An explanation of the PII, an explanation of how the PII is used, and the learning purpose for which the PII is collected and used.

Contractor shall update this information on its website as necessary to maintain accuracy.

4. Contractor shall, upon request from LCS, provide the names of Subcontractors, data elements accessible by Subcontractors, and Subcontractors use or planned use of sharing PII.

#### J. Exclusions:

This Addendum does not:

1. Impose a duty on a provider of an interactive computer service, as defined in 47 U.S.C Sec. 230, to review or enforce compliance with this Contract.
2. Impede the ability of a student to download, export, or otherwise save or maintain his or her own PII or documents.
3. Limit internet service providers from providing internet connectivity to public schools

or to students and their families.

4. Prohibit a Contractor from marketing educational products directly to parents so long as the marketing does not result from the use of PII obtained by the Contractor as a result of providing its services under this Contract.
5. Impose a duty on a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this Contract on that software or those applications.

K. This Addendum does not prohibit Contractor's use of PII to:

1. Use adaptive learning or design personalized or customized education, so long as Contractor has agreed to the transparency requirements of this Agreement.
2. Maintain, develop, support, improve, or troubleshoot a Contractor's website, online service, online application, or mobile application.
3. Provide recommendations for school, education, or employment purposes, provided Contractor does not receive any payment or other consideration from a third party to make or support the recommendation.
4. Respond to a student's request for information or feedback provided Contractor does not receive any payment or other consideration from a third party for the information or feedback.
5. Identify, for a student, institutions of higher education or scholarship providers that are seeking students who meet specific criteria, only if Contractor has obtained the written consent of the student or the student's parent or legal guardian. Contractor may use PII for this purpose regardless of whether the institutions of higher education or scholarship providers provide payment or other consideration to the Contractor.
6. In accordance with the terms of this Contract, produce and distribute, free or for payment or other consideration, student class photos and yearbooks only to LCS, students, parents, or individuals authorized by parents.
7. Provide for the student, only with the express written consent of the student or the student's parent or legal guardian given in response to clear and conspicuous notice, access to employment opportunities, educational scholarships or financial aid, or postsecondary education opportunities, regardless of whether the Contractor receives payment or other consideration from one or more third parties in exchange for the PII. This exception applies only to Contractors that provide nationally recognized assessments that postsecondary institutions of higher education use in making admissions decisions.

**THE PARTIES HERETO HAVE EXECUTED THIS ADDENDUM**

**Persons signing for Contractor hereby swear and affirm that they are authorized to act on Contractor's behalf and acknowledge that LCS is relying on their representations to that effect.**

**CONTRACTOR**

By: \_\_\_\_\_  
Name of Authorized Individual

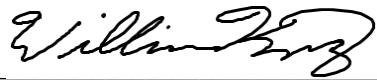
Title: \_\_\_\_\_  
Official title of Authorized Individual

\_\_\_\_\_  
\*Signature  
Date: \_\_\_\_\_

**LCS**

By: William Kranz  
Name of Authorized Individual

Title: Director of IT  
Official title of Authorized Individual

  
\_\_\_\_\_  
\*Signature  
Date: 6/20/2019

# Exhibit B

# Terms of Service

## What is a “Terms of Service” agreement?

“Terms of Service” is a legal contract/agreement between you and a service provider. It protects your rights and our rights relating to the provision of the Service, so please review these Terms carefully.

Therefore, this document is an agreement between you or the organization that you represent (hereinafter “You” or “Your”) and DonorPerfect (a division of SofterWare, Inc.) (hereinafter “DonorPerfect”) governing your use of the DonorPerfect online database, fundraising solution and any other offered services. SofterWare US headquarters is located at 601 Office Center Dr, Suite 200, Fort Washington, PA 19034 and our international offices are located at A312-1001 Lenoir Street, Montreal, QC, H4C 2Z6, and DonorPerfect UK Ltd., 33 Mabels Furlong, Ledbury, HR8 2HQ, United Kingdom.

## Parts of this Agreement

This Agreement consists of the following terms and conditions (hereinafter the “General Terms”) and terms and conditions, if any, specifically to the use of individual services (hereinafter the “Service Specific Terms”). The General Terms and Service Specific Terms are collectively referred to as the “Terms”. In the event of a conflict between the General Terms and Service Specific Terms, the Service Specific Terms shall prevail.

## Acceptance of the Terms

You must be of legal age to enter into a binding agreement in order to accept the Terms. If you do not agree to the General Terms, do not use any of our services. If you agree to the General Terms and do not agree to any Service Specific Terms,

please do not use the corresponding Service. You can accept the Terms by checking a checkbox or clicking on a button indicating your acceptance of the terms or by actually using the services.

# GENERAL AND SERVICE-SPECIFIC TERMS

## Description of Service

We provide an array of services for online fundraising and management including fundraising database access, word processor, report writer, email client, mobile application, chat, donor relationship management applications and online donation payment processing applications (“service” or “services”). You may use the services for your personal and business use or for internal business purpose in the organization that you represent. You may connect to the services using any Internet browser or mobile application supported by the services. You are responsible for obtaining access to the Internet and the equipment necessary to use the services. You can create and edit content with your user account and if you choose to do so, you can publish and share such content.

## Beta Services

We may offer certain services that are initial deployments of new features called beta services (“Beta Service” or “Beta services”) for the purpose of testing and evaluation. You agree that we have the sole authority and discretion to determine the period of time for testing and evaluation of Beta services. We will be the sole judge of the success of such testing and the decision, if any, to offer the Beta services as commercial services. We may charge for Beta services but will communicate the charges in advance. You will be under no obligation to acquire a subscription to use any paid service as a result of your subscription to any Beta service. We reserve the right to fully or partially discontinue, at any time and from time to time, temporarily or permanently, any of the Beta services with or without notice to you. You agree that DonorPerfect will not be liable to you or to any third party for any harm related to,

arising out of, or caused by the modification, suspension or discontinuance of any of the Beta services for any reason.

## Modification of Terms of Service

We may modify the Terms upon notice to you at any time through a service announcement or by sending email to your primary email address. If we make significant changes to the Terms that affect your rights, you will be provided with at least 30 days advance notice of the changes by email to your primary email address. You may terminate your use of the services by providing DonorPerfect notice by email (within 30 days of being notified) if the Terms are modified in a manner that substantially affects your rights in connection with use of the services. In the event of such termination, you will be entitled to the prorated refund of the unused portion of any prepaid fees. Your continued use of the service after the effective date of any change to the Terms will be deemed to be your agreement to the modified Terms.

## User Sign up Obligations

You need to sign up for a user account by providing all required information in order to access or use the services. If you represent an organization and wish to use the services for corporate internal use, we recommend that you, and all other users from your organization, sign up for user accounts by providing your organization's contact information. In particular, we recommend that you use your organization email address. You agree to: a) provide true, accurate, current and complete information about yourself as prompted by the sign-up process; and b) maintain and promptly update the information provided during sign up to keep it true, current, and complete. If you provide any information that is untrue, outdated, or incomplete, or if DonorPerfect has reasonable grounds to suspect that such information is untrue, outdated, or incomplete, DonorPerfect may terminate your user account and refuse current or future use of any or all of the services.

## Conflict of Interest

You agree that you will disclose to DonorPerfect in writing (email, mail, or fax is acceptable) any conflicts of interest or potential conflicts of interest (e.g., work for or associate with other nonprofit software providers, electronic payment providers, payment processors, etc.) you may have in a timely manner. You must also disclose whether you are an employee, contractor, an employee of a contractor, or have a business/personal relationship with anyone of the above types of organizations or any of the following companies or their subsidiaries:

- Blackbaud
- FrontStream
- Kindful

Your use of DonorPerfect may not be used for competitive research, and you agree that neither your organization, nor any person accessing the services by means of your organization's account, will, directly or indirectly, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the services; modify, translate or create derivative works based on the services; or rent, lease, distribute, assign or otherwise transfer rights to the services.

Failure to disclose any of these relationships in writing or using DonorPerfect for competitive research may result in legal action against you and/or your organization, including financial damages, to the fullest extent allowed by law.

## Organization Accounts and Administrators

When you sign up for an account for your organization you may specify one or more administrators. The administrators will have the right to configure the services based on your requirements and manage end users in your organization account. If your organization account is created and configured on your behalf by a third party, it is likely that such third party has assumed administrator role for your organization. Make sure that you enter into a suitable agreement with such third party specifying such party's roles and restrictions as an administrator of your organization account. You are responsible for i) ensuring confidentiality of your organization account password, ii) appointing competent individuals as administrators for managing your



organization account, and iii) ensuring that all activities that occur in connection with your organization account comply with this Agreement. You understand that DonorPerfect is not responsible for account administration and internal management of the services for you. You are responsible for taking necessary steps for ensuring that your organization does not lose control of the administrator accounts. DonorPerfect may provide control of an administrator account to an individual providing proof satisfactory to DonorPerfect demonstrating authorization to act on behalf of the organization. You agree not to hold DonorPerfect liable for the consequences of any action taken by DonorPerfect in good faith in this regard.

## Personal Information and Privacy

Personal information you provide to DonorPerfect through the service is governed by DonorPerfect Privacy Policy. Your election to use the service indicates your acceptance of the terms of the [DonorPerfect Privacy Policy](#). You are responsible for maintaining the confidentiality of your username, password and other sensitive information. You are responsible for all activities that occur in your user account and you agree to inform us immediately of any unauthorized use of your user account by email to [legal@donorperfect.com](mailto:legal@donorperfect.com) or by calling us at US (800) 220-8111. We are not responsible for any loss or damage to you or to any third party incurred as a result of any unauthorized access and/or use of your user account, or otherwise.

## Communications from DonorPerfect

The service may include certain communications from DonorPerfect, such as service announcements, administrative messages and newsletters. You understand that these communications shall be considered part of using the services. As part of our policy to provide you total privacy, we also provide you the option of opting out from receiving newsletters from us. However, you will not be able to opt-out from receiving service announcements and administrative messages.

## Fees and Payments

The services are available under subscription plans of various durations. Payments for subscription plans of a duration of less than a year can be made only by Credit Card or Direct Debit/ACH bank account withdrawal. Your subscription will be automatically renewed at the end of each subscription period unless you downgrade your paid subscription plan to a free plan, if available, or inform us that you do not wish to renew the subscription. At the time of automatic renewal, the subscription fee will be charged to the Credit Card or Direct Debit/ACH bank account last used by you. We provide you the option of changing the details if you would like the payment for the renewal to be made through a different Credit Card or Direct Debit/ACH bank account. If you do not wish to renew the subscription, you must inform us at least seven (7) days prior to the renewal date. If you have not downgraded to a free plan and if you have not informed us that you do not wish to renew the subscription, you will be presumed to have authorized DonorPerfect to charge the subscription fee to the Credit Card or Direct Debit/ACH bank account last used by you. Prepayments are nonrefundable as we must allocate resources for your guaranteed use of the services.

From time to time, we may change the price of any service or charge for use of services that are currently available free of charge. Any increase in charges will not apply until the expiration of your then-current billing cycle. You will not be charged for using any service unless you have opted for a paid subscription plan.

## Restrictions on Use

In addition to all other terms and conditions of this Agreement, you shall not: (i) transfer the services or otherwise make it available to any third party; (ii) provide any service based on the services without prior written permission; (iii) use the third party links to sites without agreeing to their website terms & conditions; (iv) post links to third party sites or use their logo, company name, etc. without their prior written permission; (v) publish any personal or confidential information belonging to any person or entity without obtaining consent from such person or entity; (vi) use the services in any manner that could damage, disable, overburden, impair or harm any server, network, computer system, resource of DonorPerfect; (vii) violate any applicable local, state, national or international law; and (viii) create a false identity to mislead any person as to the identity or origin of any communication.

# Illegal Activities and/or Spamming

You agree to be solely responsible for the contents of your transmissions through the services. You agree not to use the services for illegal purposes or for the transmission of material that is unlawful, defamatory, harassing, libelous, invasive of another's privacy, abusive, threatening, harmful, vulgar, pornographic, obscene, or is otherwise objectionable, offends religious sentiments, promotes racism, contains viruses or malicious code, or that which infringes or may infringe intellectual property or other rights of another. You agree not to use the services for the transmission of "junk mail", "spam", "chain letters", "phishing" or unsolicited mass distribution of email. We reserve the right to terminate your access to the services if there are reasonable grounds to believe that you have used the services for any illegal or unauthorized activity.

# Application Programming Interface

This section does not apply if you do not request access to DonorPerfect's application programming interface, which is an interface to push data to or pull data from your DonorPerfect database (the "API") over the internet. The API may only be licensed to you upon submission of an application along with any requested information and receipt of DonorPerfect's approval, which may be granted or denied in DonorPerfect's sole discretion. If DonorPerfect provides you with access to the API, it will be deemed to be included in the "services" for purposes of this Agreement, except that any consulting services, support or other assistance requested by you relating to the API are not included in any Fees unless expressly stated in writing. DonorPerfect may limit the amount of data that may be transferred by you through the use of the API, the number of concurrent sessions that you may establish with the API, and/or any other activity with respect to the API, in DonorPerfect's sole discretion and may change such limitations from time to time. DonorPerfect also reserves the right to terminate your license to use the API at any time after such license is granted if DonorPerfect believes you are using the API in an inappropriate manner. The API shall be treated by you as confidential information of DonorPerfect. Any breach of the foregoing restrictions (or this Agreement) by any third party service provider you use shall be deemed a breach of this Agreement by you.

# DPCConnect Marketplace and Acquisition of Non-DonorPerfect Products or Services

We or third parties may make available (for example, through the [DPCConnect Marketplace](#) or otherwise) third-party products or services, including, for example, non-DonorPerfect applications and implementation and other consulting services. Any acquisition by you of such products or services, and any exchange of data between you and any non-DonorPerfect provider, is solely between you and the applicable non-DonorPerfect provider. We do not warrant or support non-DonorPerfect applications or other non-DonorPerfect products or services, whether or not they are designated by us as “certified”, “featured”, or otherwise, except as specified in a signed proposal from us. If you install or enable a non-DonorPerfect application for use with any of our services, you grant us permission to allow the provider of that non-DonorPerfect application to access your data as required for the interoperation of that non-DonorPerfect application with the services we provide. We are not responsible for any disclosure, modification or deletion of your data resulting from access by a non-DonorPerfect application. Our services may contain features designed to integrate with Non-DonorPerfect applications. To use such features, you may be required to obtain access to non-DonorPerfect applications from their providers, and may be required to grant us access to your account(s) on the non-DonorPerfect applications. If the provider of a non-DonorPerfect application ceases to make the non-DonorPerfect application available for interoperation with the corresponding service features on a reasonable term or basis, we may cease providing those service features without entitling you to any refund, credit, or other compensation.

## Termination and Inactive User Accounts Policy

We reserve the right to terminate unpaid user accounts that are inactive for a continuous period of 180 days. For paid user accounts, we will terminate user accounts that are delinquent for a continuous period of 21 days past the last payment

due date. In the event of any termination, all data associated with such user account will be deleted. We will provide you prior notice of such termination, and you can backup your data by using the service(s) or we can provide a backup of your data in electronic format for a fee equal to two (2) months of service or \$250.00, whichever is higher, or you can elect in writing to have DonorPerfect keep your data protected on our servers without access rights for a stated time period for 1/2 of your fee minus additional support or other modules that you are no longer using. The data deletion policy may be implemented with respect to any or all of the services. Each service will be considered an independent and separate service for the purpose of calculating the period of inactivity. In other words, activity in one of the services is not sufficient to keep your user account in another service active. In case of accounts with more than one user, if at least one of the users is active, the account will not be considered inactive.

## Data Ownership

We respect your right to ownership of content created or stored by you. You own the content created or stored by you. Unless specifically permitted by you, your use of the services does not grant DonorPerfect the license to use, reproduce, adapt, modify, publish or distribute the content created by you or stored in your user account for DonorPerfect's commercial, marketing or any similar purpose, except for i) Non-identifiable summary and transaction details which DonorPerfect may use and share with the greater nonprofit community, media, and interested third parties and ii) DonorPerfect's permission to access, copy, distribute, store, transmit, reformat, publicly display and publicly perform the content of your user account as required for the purpose of providing the services to you and supporting the services to you through email, chat, telephone, or any other communication means.

You agree and acknowledge that when accessing the services, DonorPerfect also receives and stores certain personally non-identifiable information. Such information, which is collected passively using various technologies, cannot be used to specifically identify you. DonorPerfect may store such information itself or such information may be included in databases owned and maintained by DonorPerfect affiliates, agents or service providers. DonorPerfect may use such information and pool it with other information to track, for example, the total number of visitors or users of the services, the average donation of visitors to its online donation forms, the number of visitors to

each page of DonorPerfect website, the domain names of DonorPerfect visitors' Internet service providers, and how DonorPerfect users use and interact with the service. All aggregated and non-identifiable information can be used by DonorPerfect to create and improve our products and services. Also, in an ongoing effort to better understand and serve the users of the services, DonorPerfect may conduct research on its customer demographics, interests and behavior based on the Contact Data and other information provided to DonorPerfect. This research may be compiled and analyzed on an aggregate basis. DonorPerfect may share this non-identifiable and aggregate data with its affiliates, agents and business partners, but this type of non-identifiable and aggregate information does not identify you personally. DonorPerfect may also disclose aggregated user statistics in order to describe DonorPerfect services to current and prospective business partners and to other third parties for other lawful purposes.

## Confidential Information

Neither party will disclose, sell or transfer to any third party, other than for the performance of this Agreement, any Confidential Information of the other party without the express, prior written consent of the other party. Confidential information shall mean information including, without limitation, computer programs, code, algorithms, know-how, formulas, processes, ideas, inventions (whether patentable or not), and information marked "Confidential", or if disclosed verbally, is identified as confidential at the time of disclosure but does not include information (1) generally known to the public, (2) already known to the party receiving the information, or (3) legally obtained from a third party without further duties of confidentiality.

DonorPerfect will use commercially available security software for encrypting the transmission of your Data. "Data" shall mean the data inputted by you, Authorized Users, or DonorPerfect on your behalf for the purpose of using the services or facilitating your use of the services. You acknowledge that transmission of data over the Internet may not be secure, however, even after reasonable security measures have been taken.

## User Generated Content

You may transmit or publish content created by you using any of the services. However, you shall be solely responsible for such content and the consequences of its transmission or publication. Any content made public will be publicly accessible through the internet and may be crawled and indexed by search engines. You are responsible for ensuring that you do not accidentally make any private content publicly available. Any content that you may receive from other users of the services, is provided to you AS IS for your information and personal use only and you agree not to use, copy, reproduce, distribute, transmit, broadcast, display, sell, license or otherwise exploit such content for any purpose, without the express written consent of the person who owns the rights to such content. In the course of using any of the services, if you come across any content with copyright notice(s) or any copy protection feature(s), you agree not to remove such copyright notice(s) or disable such copy protection feature(s) as the case may be. By making any copyrighted/copyrightable content available on any of the services you affirm that you have the consent, authorization or permission, as the case may be from every person who may claim any rights in such content to make such content available in such manner. Further, by making any content available in the manner aforementioned, you expressly agree that DonorPerfect will have the right to block access to or remove such content made available by you if DonorPerfect receives complaints concerning any illegality or infringement of third party rights in such content. By using any of the services and transmitting or publishing any content using such service, you expressly consent to determination of questions of illegality or infringement of third party rights in such content by the agent designated by DonorPerfect for this purpose.

## Trademark

DonorPerfect, DonorPerfect logo, the names of individual services and their logos are trademarks of SofterWare, Inc. You agree not to display or use, in any manner, the DonorPerfect trademarks, without DonorPerfect's prior written permission.

## Disclaimer of Warranties

YOU EXPRESSLY UNDERSTAND AND AGREE THAT THE USE OF THE SERVICES IS AT YOUR SOLE RISK. THE SERVICES ARE PROVIDED ON AN AS-IS AND AS-AVAILABLE BASIS. DONORPERFECT EXPRESSLY

DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. DONORPERFECT MAKES NO WARRANTY THAT THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE. USE OF ANY MATERIAL DOWNLOADED OR OBTAINED THROUGH THE USE OF THE SERVICES SHALL BE AT YOUR OWN DISCRETION AND RISK AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM, MOBILE TELEPHONE, WIRELESS DEVICE OR DATA THAT RESULTS FROM THE USE OF THE SERVICES OR THE DOWNLOAD OF ANY SUCH MATERIAL. NO ADVICE OR INFORMATION, WHETHER WRITTEN OR ORAL, OBTAINED BY YOU FROM DONORPERFECT, ITS EMPLOYEES OR REPRESENTATIVES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

## Limitation of Liability

YOU AGREE THAT DONORPERFECT SHALL, IN NO EVENT, BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR OTHER LOSS OR DAMAGE WHATSOEVER OR FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, COMPUTER FAILURE, LOSS OF BUSINESS INFORMATION, OR OTHER LOSS ARISING OUT OF OR CAUSED BY YOUR USE OF OR INABILITY TO USE THE SERVICE, EVEN IF DONORPERFECT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. IN NO EVENT SHALL DONORPERFECT'S ENTIRE LIABILITY TO YOU IN RESPECT OF ANY SERVICE, WHETHER DIRECT OR INDIRECT, EXCEED THE LAST TWELVE (12) MONTHS OF FEES PAID BY YOU TOWARDS SUCH SERVICE.

## Indemnification

You agree to indemnify and hold harmless DonorPerfect, its officers, directors, employees, suppliers, and affiliates, from and against any losses, damages, fines and expenses (including attorney's fees and costs) arising out of or relating to any claims that you have used the services in violation of another party's rights, in violation of



any law, in violations of any provisions of the Terms, or any other claim related to your use of the services, except where such use is authorized by DonorPerfect.

Where such use is authorized by DonorPerfect, DonorPerfect shall defend, indemnify and hold you harmless from any and all claims, costs, damages, judgments and reasonable attorney's fees resulting from or arising out of DonorPerfect's material breach with its agreements with third parties provided that: (a) you promptly notify DonorPerfect of any event requiring indemnification promptly following your discovery of third party claims, promptly following the receipt of notice of the commencement of any action or proceeding; (b) DonorPerfect shall have sole control of the defense, and compromise and defend any third party action or proceeding in connection with which indemnification is sought; and (c) you shall cooperate with DonorPerfect with respect to such defense and settlement. Finally, you shall have the right to participate at your own expense in any such action or proceeding.

## Arbitration

Any controversy or claim arising out of or relating to the Terms shall be settled by binding arbitration in accordance with the commercial arbitration rules of the American Arbitration Association, or for any non-United States of America based organizations, the Association for International Arbitration. Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The decision of the arbitrator shall be final and unappealable. The arbitration shall be conducted in the State of Pennsylvania, United States of America, and judgment on the arbitration award may be entered into any court having jurisdiction thereof. Notwithstanding anything to the contrary, DonorPerfect may at any time seek injunctions or other forms of equitable relief from any court of competent jurisdiction.

## Suspension and Termination

We may suspend your user account or temporarily disable access to whole or part of any service in the event of any suspected illegal activity, extended periods of inactivity or requests by law enforcement or other government agencies. Objections to suspension or disabling of user accounts should be made

to [legal@donorperfect.com](mailto:legal@donorperfect.com) within thirty days of being notified about the suspension. We may terminate a suspended or disabled user account after thirty days. We will also terminate your user account on your request. In addition, we reserve the right to terminate your user account and deny the services upon reasonable belief that you have violated the Terms and to terminate your access to any Beta service in case of unexpected technical issues or discontinuation of the Beta service. You have the right to terminate your user account if DonorPerfect breaches its obligations under these Terms and in such event, you will be entitled to prorated refund of any prepaid fees. Termination of user account will include denial of access to all services, deletion of information in your user account such as your email address and password and deletion of all data in your user account.

## End of Terms of Service

If you have any questions or concerns regarding this Agreement, please contact us at [legal@donorperfect.com](mailto:legal@donorperfect.com).

<https://www.donorperfect.com/company/terms-of-service/> - pulled from here on 8/11/2019

# Exhibit C

# Privacy Statement

At SofterWare, we are committed to protecting your privacy. This privacy policy statement provides you with information regarding our information gathering and usage practices for our websites and services.

## Your Personal Information

SofterWare and its websites, including those operating at SofterWare.com, DonorPerfect.com, DonorPerfect.net, EZCareSoftware.com, and ReadySetAuction.com offer several opportunities for visitors to register for promotional and informational mailings, and to receive assistance in evaluating our software and services. We do not collect any personal information about visitors to our websites unless they choose to provide it voluntarily. We define “personal information” as information that personally identifies an individual or allows us to contact you. Such information might include a phone number, name or email address.

We also provide online tools that our customers use to operate aspects of their business or organization for purposes of fundraising, customer relationship management, childcare centers or camp operations, online donation and auction services, and social engagement among others. In providing these tools, SofterWare processes data our customers or their constituents submit to our services, or instruct us to process on their behalf. While SofterWare’s customers or their constituents decide what data to submit, it typically includes information about their constituents, donations, and contact information.

Information submitted to us is only available to employees for purposes of contacting customers, sending materials based on their requests for information, providing news and relevant information about our company, or supporting our products and services that our customers utilize. We also use this information to help us determine their needs related to our software solutions.

Users may opt out of receiving future mailings at any time by sending an email to [info@softerware.com](mailto:info@softerware.com).

## We Operate in the United States

We have servers and offices located in the United States, so your information may be transferred to, stored, or processed in the United States. While the data protection, privacy, and other laws of

the United States might not be as comprehensive as those in your country, we adhere to the United States / European Union Privacy Shield Arrangement. You can find more information on the Privacy Shield program by visiting <https://www.privacyshield.gov/>. By using our Websites, you understand and consent to the collection, storage, processing, and transfer of your information to our facilities in the United States and those third parties with whom we share it as described in this policy and the “[EU-US Privacy Shield Information](#)” section listed below.

## Sharing and Usage

SofterWare will not sell, share, rent, or disclose your personal information without your advance permission or unless ordered by a court of law. We occasionally contract with other companies to provide limited services on our behalf for the purposes of providing and improving our services, or serving you better. Examples of such services might include (but are not limited to) mailing services, data de-duplication services and address verification services. We will provide those companies only the information they need to deliver the service, and they are prohibited from using that information for any other purpose.

## IP Information Tracked

We use your IP address to administer our web site, help diagnose problems with our servers, and to identify the general geographic region of the device in order to provide the most efficient service capacity to that region. An IP address is a unique identifier used by devices to identify and communicate with each other on the Internet. IP addresses are not linked to personally identifiable information. We track browser types and versions to help us understand our visitors’ needs related to our web site design. We currently do not process Do Not Track signals sent by your Internet browser because a universal technology standard has not yet been fully established.

## Cookies

Cookies are small alphanumeric identifiers created by your browser on your system when you visit a website. They do not gather or provide personally identifiable information. We use cookies to enable our systems to recognize your browser and ensure a fluid, secure, and consistent user experience. Client-side cookies store preferences, identify where you are in a process, help to prevent you from entering information repeatedly, and provide page usage statistics in order for us to provide an optimal experience. We also use cookies to track and measure the success of our website and marketing campaigns in meeting your informational needs. Additionally, visitors that entered our sites by responding to a Google Adwords

Advertisement may be associated with a site conversion in Google's advertising tracking tool. If a user rejects the cookie, he may still use our site; however, the user's access to some areas or functionality within our website may be limited.

## Security

We take the security of our systems very seriously and take appropriate measures to ensure it remains safe. While no website can guarantee security, we maintain appropriate technical and procedural safeguards to protect your personal information. SofterWare, Inc. takes care to reinforce the importance of our web site visitors' security and privacy among our employees.

## Choice/Opt-out

You may opt in and opt out of receiving communications from us by sending an e-mail to [info@softerware.com](mailto:info@softerware.com).

## Notification of Changes

We will post any changes to this privacy statement on [www.softerware.com/privacy-policy](http://www.softerware.com/privacy-policy).

## EU-US Privacy Shield Information

For more information on the EU-US Privacy Shield program, or to view a list of participating companies, visit <https://www.privacyshield.gov/welcome>.

## SofterWare Privacy Shield Notice

SofterWare, Inc. and all of its controlled U.S. subsidiaries ("SofterWare") are committed to protecting your privacy. We have prepared this Privacy Policy to describe to you our practices regarding the Personal Data (as defined below) we collect from users of our websites, including those located at SofterWare.com, DonorPerfect.com, DonorPerfect.net, EZCareSoftware.com, and ReadySetAuction.com.

SofterWare complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. SofterWare has certified that it adheres to the Privacy Shield Principles. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit <https://www.privacyshield.gov/>.

SofterWare’s participation in the Privacy Shield applies to all personal data that is subject to the Privacy Shield Principles and is received from the European Union. SofterWare will comply with the Privacy Shield Principles in respect of such personal data.

For purposes of this Notice, “Personal Data” means information that (i) is transferred from the EU to the United States, (ii) is recorded in any form, (iii) is about, or relates to, an identified or identifiable consumer, customer, supplier or other individual, and (iv) can be linked to that consumer, customer supplier or other individual. This Notice outlines our general policy and practices for implementing the Privacy Shield principles for Personal Data.

## **Privacy Shield Principles**

SofterWare’s practices regarding the collection, storage, transfer, use and other processing of Personal Data comply with the Privacy Shield principles of notice, choice, onward transfer, access, security, data integrity, and enforcement and oversight.

## **Notice**

We notify our consumers, customers, suppliers and others located in the EU about the purposes for which we collect and use Personal Data, the types of third parties to which we disclose the information, the choices consumers, customers, suppliers and others have for limiting the use and disclosure of their information, and how to contact us about our practices concerning Personal Data.

When we receive Personal Data from our customers, affiliates or other entities in the EU we will use and disclose such information in accordance with the notices provided by such entities and the choices made by the individuals to whom such Personal Data relates.

## **Purpose of Collection and Use of Personal Data**

SofterWare collects certain Personal Data such as name, email address, postal address and telephone number. We do not collect sensitive Personal Data of consumers, customers or suppliers, such as information about medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or other sensitive information as defined by the Privacy Shield framework.

We use Personal Data of consumers, customers, suppliers and others (i) to respond to their requests, (ii) to evaluate the quality of our products and services, (iii) to communicate with them about our products, services and related issues, (iv) to notify them of and administer offers and promotions, (v) for internal administrative and analytics purposes, and (vi) to comply with our legal obligations, policies and procedures.

## Choice

SofterWare shares Personal Data with its service providers. With respect to Personal Data we share with other third parties, we provide consumers, customers, suppliers and others located in the EU with an opportunity to opt-out of such sharing. You can opt-out by sending an email to [legal@softerware.com](mailto:legal@softerware.com). We do not use Personal Data for purposes incompatible with the purposes for which the information was originally collected without notifying the relevant consumers, customers, suppliers and others of such uses and offering an opportunity to opt-out.

In addition, we may disclose Personal Data (i) if we are required to do so by law or legal process, (ii) to law enforcement authorities or other government officials based on an enforceable governmental request or as may be required under applicable law, or (iii) when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss or in connection with an investigation of suspected or actual illegal activity.

## Onward Transfer of Personal Data

We may share Personal Data with service providers we have retained to perform services on our behalf. We now require service providers to whom we disclose Personal Data and who are not subject to laws based on the European Union Data Protection Directive to either subscribe to the Privacy Shield principles or agree to provide at least the same level of protection for Personal Data as is required by the relevant Privacy Shield principles. If the third party does not comply with its privacy obligations, SofterWare will take commercially reasonable steps to prevent or stop the use or disclosure of Personal Data. In the context of an onward transfer, SofterWare has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. SofterWare shall remain liable under the Principles if its agents that it engages to process such personal information do so in a manner inconsistent with the Principles, unless SofterWare proves that it is not responsible for the event giving rise to the damage.

## Access to Personal Data



SofterWare provides consumers, customers, suppliers and others with reasonable access to the Personal Data maintained about them. We also provide a reasonable opportunity to correct, amend or delete that information where it is inaccurate. We may limit or deny access to Personal Data where providing such access is unreasonably burdensome or expensive under the circumstances, or as otherwise permitted by the Privacy Shield principles. To obtain access to Personal Data, consumers, customers, suppliers and others may contact SofterWare as specified in the “How to Contact Us” section of this Policy.

## **Security**

SofterWare maintains reasonable administrative, technical and physical safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction.

## **Data Integrity**

SofterWare takes reasonable steps to ensure that Personal Data collected by SofterWare is relevant for the purposes for which it is to be used and that the information is reliable for its intended use and is accurate, complete and current. We depend on our consumers, customers, suppliers and others to update or correct their Personal Data whenever necessary.

## **Your Rights to Access, to Limit Use, and to Limit Disclosure**

EU individuals have rights to access personal data about them, and to limit use and disclosure of their personal data. With our Privacy Shield certification, SofterWare has committed to respect those rights. Because in some circumstances SofterWare personnel have limited ability to access data our customers submit to our services, if you wish to request access, to limit use, or to limit disclosure, please provide the name of the SofterWare customer who submitted your data to our services. We will refer your request to that customer, and will support them as needed in responding to your request.

## **Compelled Disclosure**

SofterWare may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

## Inquiries and Complaints

In compliance with the Privacy Shield Principles, SofterWare commits to resolve complaints about your privacy and our collection or use of your personal information. European Union individuals with inquiries or complaints regarding this privacy policy should first contact SofterWare at [legal@softerware.com](mailto:legal@softerware.com) or at the mailing address shown below.

### SofterWare

Attention: Law Department  
601 Office Center Dr, Suite 200, Fort Washington, PA 19034  
USA

**SofterWare will respond within 45 days.** If we fail to respond within that time, or if our response does not address your concern, you may contact ICDR/AAA (<https://www.icdr.org>), which provides an independent third-party dispute resolution body based in the United States. The services of ICDR/AAA are provided at no cost to you. If neither SofterWare nor ICDR/AAA resolves your complaint, you may have the possibility to engage in binding arbitration through the Privacy Shield Panel. Also, SofterWare's commitments under the Privacy Shield are subject to the investigatory and enforcement powers of the United States Federal Trade Commission.

## How to Contact Us

You may address any questions or concerns regarding our Privacy Shield Policy or our practices concerning Personal Data by:

Contacting us through our website: [Click here](#), or

**Writing to:**

SofterWare  
Attention: Law Department  
601 Office Center Dr, Suite 200, Fort Washington, PA 19034  
USA

## Amendment

The SofterWare Privacy Shield Notice may be amended from time-to-time in compliance with the requirements of the Privacy Shield principles. Appropriate notice will be given concerning such amendments.

This Privacy Shield Notice is effective as of April 2nd, 2017