ACD Direct

Data Processing and Security Terms (Customers)

Policy Version v1.0

Revision History

Version	*Date*	*Author*	*Description of Change*
1.1	4/13/2020	Louise Watson, Project Manager Shaun Beecroft, IT Infrastructure Manager	Changes after review by legal

Contents

1. Introduction

This document contains the ACD Direct information processing and security terms for customers. The customer agreeing to these terms ("CUSTOMER"), and ACD Direct, or any other entity that directly or indirectly controls, is controlled by, or is under common control with ACD Direct, have entered into an agreement under which ACD Direct is providing services.

These Data Processing and Security Terms (the “Terms”) will be effective and replace any previously applicable data processing and security terms as from the Terms Effective Date (as defined below).

These Terms supplement the Agreement. Where the Agreement was entered into offline with ACD Direct, these Terms supersede the “Privacy” Clause in that agreement (if applicable).

These Terms reflect the parties’ agreement with respect to the terms governing the processing and security of Customer Data under the Agreement.

2. Definitions

Confidential information: All information and data supplied by customer or captured on the behalf of the customer is confidential and proprietary, including, without limitation, the terms of this Agreement, Reports, caller/donor personally identifiable information and data, including without limitation caller/donor names, addresses, telephone number, e-mail address, and credit card information, customer’s financial information, including without limitation its campaigns, projects, scripts and customer’s business. “Donor Information”, as defined below, is also considered confidential information.

Data Incident means a breach of ACD Direct’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Confidential Information on systems managed by or otherwise controlled by ACD Direct. “Data Incidents” will not include unsuccessful attempts or activities that do not compromise the security of confidential information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

Donor Information specifically includes, but is not limited to, (a) the names of the Donor and Customer, (b) the address of the Donor, (c) the telephone number of the Donor, (d) the social security number or federal identification number of the Donor, (e) the amount pledged by the Donor, (f) the city or state of the Donor, and (g) the terms of the Donor's pledge. "Donor Information" constitutes any information which, if disclosed, could enable a person or entity to identify the identity of the Donor or any entity controlled by or under common control with the Donor.

Authorized User means customer-provided names and emails that will access ACD Direct’s Systems, generally employees, contractors, third party processors, database vendors, or volunteers.

Third Party Auditor means an ACD Direct-appointed, qualified and independent third-party auditor, whose then-current identity ACD Direct will disclose to Customer.

ACD Direct’s Systems means all ACD’s customer-accessed web and mobile applications including but not limited to: SimpleACD, SimpleScript, PledgeCart, SimplePledge, Mobile Canvasser, and CallsWithoutWalls.

SOC 2 means a confidential Service Organization Control (SOC) 2 report (or a comparable report) on ACD Direct’s systems examining logical security controls, physical security controls,

and system availability, as produced by ACD Direct's Third Party Auditor in relation to the Audited Services.

PCI means a confidential Payment card industry (PCI) compliance report that refers to the technical and operational standards that businesses must follow to ensure that credit card data provided by cardholders is protected, as produced by ACD Direct's Third Party Auditor in relation to the Audited Services.

Third Party Processors means third parties authorized, by CUSTOMERS, under these Terms to have logical access to and process Confidential Information in order to provide parts of the Services.

3. Security Statements & Responsibilities of Customer:

A. CUSTOMER agrees that all Confidential Information and Donor Information data supplied by CUSTOMER is supplied within CUSTOMER's sole discretion and that Donor Information is highly confidential.
B. CUSTOMERS' employees, third party processors, data vendors, contractors, and volunteers accessing ACD Direct's systems will have full access to any of the Confidential Information and Donor Information and take full responsibility for the security and quality of data entered by their own employees, third party processors, data vendors, or volunteers.
C. CUSTOMERS' will provide employees, contractors, and volunteers information for access to ACD's systems. These Authorized Users that will have password-protected access to ACD Direct's systems will not share, misuse, or otherwise make public specific usernames or passwords. CUSTOMER will notify ACD Direct when Authorized Users must have access removed.
D. CUSTOMER will ensure that all Authorized Users comply with the terms and conditions of these Terms with respect to the Services. CUSTOMER will promptly notify ACD Direct of any suspected or alleged violation of authorized access.
E. CUSTOMER acknowledges that ACD Direct will collect and process the personal data of consumers or donors, which is controlled and processed by CUSTOMER or CUSTOMER's authorized third-party processor.
F. CUSTOMER is solely responsible for responding to Consumers' and Donors' requests for access to their Confidential Information and donor information.
G. CUSTOMER is in compliance and will comply with all applicable laws, regulations, ordinances and other requirements relating to the operation of its business and the provision of the services provided, especially as it relates to PCI Compliance and the PCI Compliance of the CUSTOMER's third party processors and data vendors.

4. Security Compliance:

ACD Direct shall comply with applicable local, state and federal rules and regulation to maintain the confidentiality and safeguard Materials and Confidential Information. ACD Direct maintains Level 1 PCI Service Provider and SOC 2 Type 2 certification, audited yearly by a third-party auditor. Attestations of Compliance (AOC) available upon request.

5. Security Statements & Responsibilities of ACD:

A. ACD Direct agrees that all information and data supplied by CUSTOMER or captured on the behalf of CUSTOMER is confidential and proprietary.

B. ACD Direct agrees to keep, and to take reasonable steps to attempt to have each of its Vendors (collectively, "Acquiring Party") keep, secret all such Confidential Information of CUSTOMER and not to disclose or otherwise use such Confidential Information, except with CUSTOMER's prior written consent, to anyone outside of Acquiring Party and only to those employees who have a need-to-know, either during or after the Term.

C. ACD Direct further agrees to deliver to CUSTOMER, at any time CUSTOMER may so request, all memoranda, notes, records, databases, computer files, reports and other documents (and all copies thereof) relating to CUSTOMER's business which ACD Direct may then possess or have under its control.

D. Under no circumstances may Donor Information be used or disclosed by ACD Direct, any agent or employee of ACD Direct, or any independent contractor or vendor of ACD Direct without taking reasonable steps to obtain written authorization from CUSTOMER.

E. ACD Direct shall, at all times, keep the Donor Information and Confidential Information secure by encrypting it and/or by limiting access to Authorized Users with frequently updated password-protected access, and with passwords set through two-factor authentication (or better).

F. ACD Direct may suspend or terminate any Authorized User's access for any reason at any time.

G. ACD Direct acknowledges and agrees that under no circumstances will ACD Direct ever disclose any of the Confidential Information and Donor Information. If any demand for any Confidential Information is made by any person other than CUSTOMER, ACD Direct shall immediately notify the appropriate and designated person(s) of the CUSTOMER of the request. In the event that ACD Direct is requested or required to disclose such Confidential Information (for example, but not by limitation, through the issuance of a subpoena, a subpoena duces tecum or verbal testimony), ACD Direct shall also immediately notify CUSTOMER so as to give CUSTOMER an opportunity to file or make appropriate objections.

H. As a condition to any employee, agent, independent contractor or vendor of ACD Direct having any access to the Confidential Information, it shall first agree to be bound by these terms. ACD Direct nor any of its employees, contractors, agents, or vendors will use, misuse or misappropriate any Confidential Information and will only use such Confidential Information in the manner set forth herein in connection with rendering the services provided.

I. In the event of a Data Incident, ACD Direct will employ its Incident Response Plan. The policy is available by request at any time.

J. ACD Direct is in compliance and will comply with all applicable laws, regulations, ordinances and other requirements relating to the operation of its business and the provision of the services provided.