Updated August 15, 2022

Data Processing Addendum

Capitalized terms not defined in this Data Processing Addendum ("***DPA***") shall have the meanings set forth in the SSA.

1. Definitions

"**Agreement**" means AppDirect's Subscription Services Agreement, which governs the provision of the Services to Company, as such terms may be updated by AppDirect from time to time.

"**Customer Data**" means any Personal Data that AppDirect processes on behalf of Company, its Customers and/or its End Users as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*

"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law, the Data Protection Act 2018 and the UK General Data Protection Regulation ("**UK Data Protection Law**"), and the CCPA.

"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"EU Standard Contractual Clauses" or "**EU SCCs**" means the clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*.

"**Processing,**" "**process**", "**processes**" and "**processed**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

"**Services**" means any product or service provided by AppDirect to Company pursuant to the Agreement.

"**Sub-processor**" means any Data Processor engaged by AppDirect or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or AppDirect's Affiliates.

"**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses.

2. Relationship with the Agreement

2.1 The parties agree that this DPA shall replace any existing DPA, including the standard contractual clauses (as applicable), the parties may have previously entered into in connection with the Services.

2.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

2.3 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.4 Any claims against AppDirect or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Company further agrees that any regulatory penalties incurred by AppDirect in relation to the Customer Data that arise as a result of, or in connection with, Company's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce AppDirect's liability under the Agreement as if it were liability to the Company under the Agreement.

2.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

2.6 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

2.7 This DPA and the applicable standard contractual clauses shall terminate simultaneously and automatically with the termination or expiration of the Agreement.

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that AppDirect processes Customer Data on behalf of Company as Data Processor in the course of providing Services pursuant to the Agreement.

Part A: General Data Protection Obligations

4. Roles and Scope of Processing

4.1 **Role of the Parties**. As between AppDirect and Company, Company is the Data Controller of Customer Data, and AppDirect shall process Customer Data only as a Data Processor acting on behalf of Company. In terms of Data Protection Laws, Company remains the responsible party ("owner of the data").

4.2 **Company Processing of Customer Data**. Company agrees that (i) it shall treat Customer Data that it receives, collects or processes as part of its obligations under the Agreement, whether from AppDirect or from Customers or End Users, in accordance with Data Protection Laws; (ii) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to AppDirect; and (iii) it has provided notice and obtained

(or shall obtain) all consents and rights necessary under Data Protection Laws for AppDirect to process Customer Data and provide the Services pursuant to the Agreement and this DPA. Should third parties assert claims against AppDirect based on the collecting, processing or usage of Controller Data, Company shall indemnify AppDirect from all such claims.

4.3 **AppDirect Processing of Customer Data**. AppDirect shall process Customer Data only for the purposes described in this DPA and only in accordance with Company's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Company's complete and final instructions to AppDirect in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Company and AppDirect.

4.4 **Details of Data Processing**

Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

Duration: As between AppDirect and Company, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Company and the performance of AppDirect's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

Nature of the processing: AppDirect provides the cloud service commerce platform and the support services for the platform. The platform allows Company, its Customers and End Users accessing the platform to purchase and manage subscriptions for Products and any of their End Users to access and use the platform, as described in the Agreement.

Categories of data subjects: Any individual accessing and/or using the Services through the Company's account; and any individual whose information is stored on or collected via the Services.

Types of Customer Data: Identification and contact data (e.g. name, address, title, contact details, username etc.); financial information (e.g. credit card details, account details, payment information etc.); employment details (e.g. employer, job title, geographic location, area of responsibility etc.); order data (e.g. documentation of all orders done incl. all order data e.g. item, product, quantity, price etc.); automatic mail traffic (e.g. with order process or changes in the user structure etc.).

4.5 AppDirect will not:

Sell Customer Data. For purposes of this paragraph, "sell" shall have the meaning set forth in the CCPA.

Process Customer Data for any purposes other than for the specific purposes set forth herein. For the avoidance of doubt, AppDirect will not process Customer Data outside of the direct business relationship between Company and AppDirect.

4.6 AppDirect certifies that it understands its restrictions and obligations set forth in this DPA and will comply with them.

5. Cooperation

5.1 The Services provide Company with a number of controls that Company may use to retrieve, correct, delete or restrict Customer Data, which Company may use to assist it in connection with its obligations under the Data Protection Laws, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Company is unable to independently access the relevant Customer Data within the Services, AppDirect shall (at Company's

expense) provide reasonable cooperation to assist Company to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to AppDirect, AppDirect shall not respond to such communication directly without Company's prior authorization, unless legally compelled to do so. If AppDirect is required to respond to such a request, AppDirect shall promptly notify Company and provide it with a copy of the request unless legally prohibited from doing so.

5.2 If a law enforcement agency sends AppDirect a demand for Customer Data (for example, through a subpoena or court order), AppDirect shall attempt to redirect the law enforcement agency to request that data directly from Company. As part of this effort, AppDirect may provide Company's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then AppDirect shall give Company reasonable notice of the demand to allow Company to seek a protective order or other appropriate remedy unless AppDirect is legally prohibited from doing so.

6. Subprocessing

6.1 **Authorized Sub-processors**. Company agrees that AppDirect may engage Sub-processors to process Customer Data on Company's behalf. Company agrees that AppDirect may employ or change Sub-processors at his own discretion. AppDirect may continue to use those Sub-processors already engaged by AppDirect as at the date of this DPA.

6.2 **Sub-processor Obligations**. AppDirect shall: (i) enter into a written agreement with each Sub-processor that imposes obligations on the Sub-processor that are no less restrictive than those imposed on AppDirect under this DPA; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause AppDirect to breach any of its obligations under this DPA.

7. Security

7.1 **Security Measures**. AppDirect shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with AppDirect's security standards described in Annex A ("**Security Measures**").

7.2 **Updates to Security Measures**. Company is responsible for reviewing the information made available by AppDirect relating to data security and making an independent determination as to whether the Services meet Company's requirements and legal obligations under Data Protection Laws. Company acknowledges that the Security Measures are subject to technical progress and development and that AppDirect may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Company.

7.3 **Company Responsibilities**. Notwithstanding the above, Company agrees that except as provided by this DPA, Company is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

8. Security Reports and Audits

8.1 Company acknowledges that AppDirect is regularly audited against PCI, SOC 1 and SOC 2 standards by independent third party auditors and internal auditors, respectively. Upon request, AppDirect shall supply (on a confidential basis) a summary copy of its audit report(s) ("**Report**") to Company, so that

Company can verify AppDirect's compliance with the audit standards against which it has been assessed, and this DPA.

8.2 AppDirect shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Company, including responses to information security and audit questionnaires that are necessary to confirm AppDirect's compliance with this DPA, provided that Company shall not exercise this right more than once per year.

9. International Transfers

9.1 **Data center locations**. AppDirect may transfer and process Customer Data anywhere in the world where AppDirect, its Affiliates or its Sub-processors maintain data processing operations. AppDirect shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

9.2 **EU data transfers**: With respect to Customer Data transferred from the European Economic Area, the EU SCCs shall apply, form part of the DPA, and take precedence over the rest of the DPA as set forth in the EU SCCs. The EU SCCs shall be completed as follows:

Company acts as a controller and AppDirect acts as Customer's processor with respect to the Personal Data subject to the EU SCCs, and its Module 2 applies.

Clause 7 (the optional docking clause) is not included.

Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization). The initial list of sub-processors is available at https://www.appdirect.com/legal/appdirects-sub-processors, and AppDirect shall update that list at least 10 business days in advance of any intended additions or replacements of sub-processors.

Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

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

Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Ireland.

Annexes I and II of the EU SCCs are set forth in Annex B of the DPA.

Annex III of the EU SCCs (List of subprocessors) is inapplicable.

9.3 **UK data transfers**: With respect to Customer Data transferred from the United Kingdom, the UK SCCs shall apply, form part of the DPA, and take precedence over the rest of the DPA as set forth in the UK SCCs. The UK SCCs shall be completed as follows:

Table 1 of the UK SCCs:

The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Annex B of this DPA.

The Key Contact shall be the contacts set forth in Annex B of this DPA.

Table 2 of the UK SCCs: the Approved EU SCCs referenced in Table 2 of the UK SCCs shall be the EU SCCs as executed by the Parties pursuant to this DPA.

Table 3 of the UK SCCs: Annex 1A, 1B, and II of the UK SCCs shall be set forth in Annexes A and B of this DPA.

Table 4 of the UK SCCs: Either party may end the UK SCCs as set out in Section 19 of the UK SCCs.

9.4 **Swiss data transfers**: With respect to transfers of Customer Data that are subject to the Swiss Federal Act on Data Protection ("**FADP**"), the EU SCCs shall apply and shall be deemed to have the following differences to the extent required by the FADP:

References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

The term "member state" in the EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.

References to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

Under Annex I(C) of the EU SCCs (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EU SCCs insofar as the transfer is governed by the GDPR.

9.5 In the event that the United Kingdom or Switzerland requires the use of revised Standard Contractual Clauses that are applicable to the DPA, such revised UK or Swiss clauses shall automatically be deemed to replace any existing Standard Contractual Clauses without the need for any further action, unless AppDirect otherwise notifies Company.

9.6 **Alternative Transfer Mechanism.** The parties agree that the data export solutions identified in *Sections 9.2 – 9.4* shall not apply if and to the extent that AppDirect adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under EU Data Protection Laws, UK Data Protection Law, or the FADP) outside of the EEA, UK, or Switzerland, as applicable ("**Alternative Transfer Mechanism**"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

Part B: GDPR Obligations

10. Additional Security

10.1 **Confidentiality of processing**. AppDirect shall ensure that any person who is authorized by AppDirect to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

10.2 **Security Incident Response**. Upon becoming aware of a Security Incident, AppDirect shall notify Company without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Company.

11. Changes to Sub-processors.

11.1 A list of AppDirect's Sub-processors is available at https://www.appdirect.com/legal/appdirects-sub-processors and AppDirect shall notify Company (for which email shall suffice) if it adds or replaces Sub-processors at least 10 days prior to any such changes.

11.2 Company may object in writing to AppDirect's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Company may suspend or terminate the Agreement (without prejudice to any fees incurred by Company prior to suspension or termination).

12. Return or Deletion of Data

12.1 Upon termination or expiration of the Agreement, AppDirect shall (at Company's election) delete or return to Company all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent AppDirect is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data AppDirect shall securely isolate and protect from any further processing, except to the extent required by applicable law; any such back-up data must be deleted at regular intervals not exceeding six (6) months from the date of termination.

13. Cooperation

13.1 To the extent AppDirect is required under EU Data Protection Law, AppDirect shall (at Company's expense) provide reasonably requested information regarding the Services to enable the Company to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

Annex A - Security Measures

I. Background

A. Purpose

This document describes the security measures that AppDirect has adopted for the purpose of protecting Personal Data and information, primarily with a view to meeting pre-defined requirements of applicable data protection and privacy laws across AppDirect's services. These requirements have largely been derived from national legislation across AppDirect's services mandating the security measures for the protection of Personal Data and are intended to provide a harmonized and single standard.

Information security techniques, and the threats to security, are continually evolving. Security must therefore be continually assessed in the light of the specific circumstances at hand to determine the appropriate level of protection.

B. Definitions

In this document, the following definitions are used:

Content	means the content of an electronic communication by a user of the AppDirect services, including the content of electronic messages, such as SMS, MMS and email, and web pages requested to the extent that it is not Traffic Data, and references to Personal Data shall include Content;
Information Systems	means all systems used to access, store or otherwise Process Personal Data, including temporary files;
Location Data	means any data Processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service, geographic location derived from mobile network cell ID data, and coordinates provided by GPS, pico-cell, femto-cell or WIFI hotspots with known or presumed coordinates for the cells or hotspots to which users are connected, and references to Personal Data shall include Location Data;
Media	means a physical object likely to be Processed in an Information System and on which data may be recorded or from which they may be retrieved;
Security Document	means the document containing the Security Plan;
Security Plan	means the measures adopted to comply with these security measures;
Traffic Data	means any data Processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof, and references to Personal Data shall include Traffic Data.

All other capitalized terms not defined in these Service Measures will have the meaning assigned to them in the Data Processing Addendum.

C. Security Categories

These security measures are divided into three categories to reflect the sensitivity of different types of data: Standard, Medium and High. The data types to which these three security categories apply are described below.

1. Standard Security Measures

The standard security measures apply to all Personal Data as identified by AppDirect, including those categories of Personal Data referred to below in relation to the Medium and High categories.

2. Medium Security Measures

The medium security measures apply to Personal Data as identified by AppDirect, including those categories of Personal Data referred to below in relation to the High category:

- Enquiries or disclosures for law enforcement purposes
- Sufficient to permit an assessment of an individual's personality
- Bank account, debit, credit or other payment card information

3. High Security Measures

The high security measures apply to the following data categories as identified by AppDirect:

- Enquiries or disclosures for law enforcement purposes where such data is also Traffic Data
- Traffic Data
- Location Data
- Content

D. Order of precedence

In the event that the security measures conflict, the higher standard shall take precedence.

E. Scope

The security measures required for access to Personal Data via communications networks guarantee a level of security equivalent to that applying to local access.

II. Standard Security Measures

A. Organizational measures

1. Security Officer

A person responsible for the overall compliance with these security measures is designated as the Security Officer. This person is trained and experienced in managing information security and provided with appropriate resources to effectively ensure compliance.

2. Security Plan and Document

a. The measures adopted to comply with these security measures are subject of a Security Plan and set out in a Security Document which is kept up to date and revised whenever relevant changes are made to the Information System or to how it is organized. The Security Document records significant changes to the security measures or the Processing activities.

b. The Security Plan addresses: Security measures relating to the modification and maintenance of the system used to Process Personal Data, including development and maintenance of applications, appropriate vendor support and an inventory of hardware and soft Physical security, including security of the buildings or premises where data Processing occurs, security of data equipment and telecommunication infrastructure and environmental controls.

c. Data security mechanisms for securing the integrity and confidentiality of the data, classification of the data.

d. Security of computers and telecommunication systems including procedures for managing back-up copies, procedures dealing with computer viruses, procedures for managing signal/codes, security for software implementation, security related to databases, security for connecting systems to the Internet, inspection of circumvention of data system, mechanisms for keeping account of attempts to break system security or gain unauthorized access.

e. The Security Plan includes:

    i. a Disaster Recovery Plan which sets out: measures to minimize interruptions to the normal functioning of the system; limit the extent of any damage and disasters; enable a smooth transition of Personal Data from one computer system to another; if necessary, provide for alternative means of operating a computer system; educate, exercise and familiarize personnel with emergency procedures; provide for fast and smooth system recovery, and minimize the economic effects of any disaster event.
    ii. a Contingency Plan which addresses the following possible dangers to the system and appropriate criteria to determine when the plan will be triggered: the critical functions and systems, the strategy for protecting the system and priorities in the event the plan is activated; an inventory of relevant staff members to be called upon during an emergency, as well as telephone numbers of other relevant parties; a set of procedures for calculating the damage incurred; realistic time management plans to enable the recovery of the system; clearly allocated staff duties; possible use of alarms and special devices (e.g., air filters, noise filters); in the event of a fire, special equipment will be available (e.g., fire extinguisher, water pumps, etc.); devices or methods for determining temperature, humidity and other environmental factors (e.g., air conditioning, thermometers, etc.); special security software to detect breaches of security; special generators for dealing with power cuts; retention of copies of software or materials in other protected buildings to avoid inadvertent loss.

f. The Security Document is available to staff who have access to Personal Data and the Information Systems, and covers the following aspects:

    i. The scope, with a detailed specification of protected resources;
    ii. The measures, standards, procedures, code of conduct rules and norms to guarantee security, including for the control, inspection and supervision of the Information Systems;
    iii. The functions and obligations of staff;
    iv. The structure of files containing Personal Data and a description of the Information Systems on which they are Processed;
    v. The purposes for which the Information Systems may be used;
    vi. The procedures for reporting, managing and responding to Security Incidents;

vii. The procedures for making back-up copies and recovering data including the person who undertook the process, the data restored and, as appropriate, which data had to be input manually in the recovery process.

3. Functions and Obligations of Staff

a. Only those employees who have demonstrated honesty, integrity and discretion have access to premises where Information Systems or media containing Personal Data are located. Staff is bound by a duty of confidentiality in respect of any access to Personal Data.

b. The necessary measures are adopted to train and make staff familiar with these security measures, any relevant policies and applicable laws concerning the performance of their functions and duties in respect of the Processing of Personal Data and the consequences of any breach of these security measures.

c. The functions and obligations of staff having access to Personal Data and the Information Systems are clearly defined and documented.

d. Employees are instructed to the effect that electronic equipment should not be left unattended and made accessible during Processing sessions.

e. Physical access to areas where any Personal Data are stored is restricted to employees who have a legitimate operational need to access such data.

f. The disciplinary measures for a breach of the security plan are clearly defined and documented and communicated to staff.

B. Technical Measures

1. Authorization

a. Only those employees who have a legitimate operational need to access the Information Systems or carry out any Processing of Personal Data are authorized to do so ("Authorized Users").

b. An authorization system is used where different authorization profiles are used for different purposes.

2. Identification

a. Every Authorized User is issued a personal and unique identification code for that purpose ("User ID").

b. A User ID will not be assigned to another person, even at a subsequent time.

c. An up-to-date record is kept of Authorized Users, and the authorized access available to each, and identification and authentication procedures is established for all access to Information Systems or for carrying out any Processing of Personal Data.

3. Authentication

a. Authorized Users are allowed to Process Personal Data if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific Processing operation or to a set of Processing operations.

b. Authentication is based on a secret password associated with User ID, and which password is only known to the Authorized User; alternatively, authentication consists in an authentication device that is used and held exclusively by the person in charge of the Processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the Processing and may be associated with either an ID code or a password.

c. One or more authentication credentials are assigned to, or associated with, an Authorized User.

d. There is a procedure that guarantees password confidentiality and integrity. Passwords are stored in a way that makes them unintelligible while they remain valid. There is a procedure for assigning, distributing and storing passwords.

e. Passwords abide to industry's best practices and guidelines. Passwords are modified by the Authorized User to a secret value known only to the Authorized User when it is first used as well as periodically thereafter.

f. The instructions provided to Authorized Users lay down the obligation, as a condition of accessing the Information Systems, to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by Authorized Users are kept with due care.

g. Authentication credentials are de-activated if they have not been used for at least six months, except for those that have been authorized exclusively for technical management and support purposes.

h. Authentication credentials are also de-activated if the Authorized User is disqualified or de-authorized from accessing the Information Systems or Processing Personal Data.

i. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions are given in advance, in writing, to clearly specify the mechanisms to ensure that data or electronic equipment are available in case the person in charge of the Processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials are kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials.

4. Access Controls

a. Only Authorized Users have access to Personal Data, including when stored on any electronic or portable media or when transmitted. Authorized Users have authorized access only to those data and resources necessary for them to perform their duties.

b. A system for granting Authorized Users access to designated data and resources is used.

c. Authorization profiles for each individual Authorized User or for homogeneous sets of Authorized Users are established and configured prior to the start of any Processing in such a way as to only enable access to data and resources that are necessary for Authorized Users to perform their duties.

d. It is regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorization profiles still apply. This also includes the list of Authorized Persons drawn up by homogeneous categories of task and corresponding authorization profile.

e. Measures are put in place to prevent a user gaining unauthorized access to, or use of, the Information Systems. In particular, firewalls and intrusion detection systems reflecting the state of the art and industry best practice are installed to protect the Information Systems from unauthorized access. Measures are put in place to identify when the Information Systems have been accessed or Personal Data has been Processed without authorization, or where there have been unsuccessful attempts at the same.

f. Information systems access controls are configured to ensure authorized access.

g. Only those staff authorized in the security document are authorized to grant, alter or cancel authorized access by users to the Information Systems.

5. Management of Media

a. Information Systems and physical media storing Personal Data are housed in a secure physical environment. Measures are taken to prevent unauthorized physical access to premises housing Information Systems.

b. Appropriate instructions are issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorized access and Processing.

c. Media containing Personal Data permits the kind of information they contain to be identified, inventoried (including the time of data entry; the Authorized User who entered the data and the person from whom the data was received; and the Personal Data entered) and stored at a physical location with physical access restricted to staff that are authorized in the security document to have such access.

d. When media are to be disposed of or reused, the necessary measures are taken to prevent any subsequent retrieval of the Personal Data and other information stored on them, or to otherwise make the information intelligible or be re-constructed by any technical means, before they are withdrawn from the inventory.

e. Media containing Personal Data is erased or rendered unreadable if it is no longer used or prior to disposal.

6. Distribution of Media and Transmission

a. Media containing Personal Data are only available to Authorized Users.

b. Printing/copying Processes are physically controlled by Authorized Users, to ensure that no prints or copies containing Personal Data remain left in the printers or copying machines.

c. Media containing Personal Data or printed copies of Personal Data contain the classification mark “Confidential”.

d. Strong encryption is used to protect Personal Data that is electronically transmitted over a public network or stored on a portable device, or where there is a requirement to store or Process Personal Data in a physically insecure environment.

e. Paper documents containing Personal Data are transferred in a sealed container / envelope that indicates clearly that the document must be delivered by hand to an Authorized User.
f. When media containing Personal Data are to leave the designated premises as a result of maintenance operations, the necessary measures are taken to prevent any unauthorized retrieval of the Personal Data and other information stored on them.

g. A system for recording incoming and outgoing media is set up to permit direct or indirect identification of the kind of media, the date and time, the sender/recipient, the number of media, the kind of information contained, how they are sent and the person responsible for receiving /sending them, who must be duly authorized.

7. Preservation, Back-up copies and Recovery

a. Tools are in place to prevent the unintended deterioration or destruction of Personal Data.

b. Procedures are defined and laid down for making back-up copies and for recovering data.

c. Back-up copies are made periodically.

8. Anti-Virus and Intrusion Detection

a. Anti-virus software and intrusion detection systems are installed on the Information Systems to protect against attacks or other unauthorized acts in respect of Information Systems. Antivirus software and intrusion detection systems are updated regularly in accordance with the state of the art and industry best practice for the Information Systems concerned.

9. Software Updates

a. The software, firmware and hardware used in the Information Systems are reviewed regularly in order to detect vulnerabilities and flaws in the Information Systems and resolve such vulnerabilities and flaws. This review is carried out at least annually.

10. Record Keeping

a. Access Record
A history of Authorized Users' access to or disclosure of Personal Data is recorded on a secure audit trail.

b. Physical Access Record
Only those staff duly authorized in the security document have physical access to the premises where Information Systems and media storing Personal Data are stored. A record of staff who access such premises is maintained, including name, date and time of access.

c. Record of Security Incidents
There is a procedure for reporting, responding to and managing Security Incidents. This includes:

i. A procedure for reporting such Security Incidents to appropriate management within AppDirect;
ii. A clearly designated team for managing and coordinating the response to a Security Incident led by the Security Officer;
iii. A documented and tested process for managing the response to a Security Incident including the requirement to keep appropriate issues and action logs to

include the time at which the Security Incident occurred, the person reporting the Security Incident, to whom it was reported and the effects thereof.

III. Medium Security Measures

A. Technical Measures

1. Identification and Authentication

a. Passwords are modified at least every 90 days.

b. The software, firmware and hardware used in the Information Systems are reviewed at least every six months in order to detect vulnerabilities and flaws in the Information Systems and resolve such vulnerabilities and flaws.

c. Mechanisms are set up to permit unequivocal, personalized identification of any user who attempts to access the information system and a check to establish whether each user is authorized.

d. Limits are placed on the scope for repeating attempts to gain unauthorized access to the Information System. After, at most, 5 failed attempts to authenticate, the associated User ID must be blocked.

2. Tests with Real Data

a. Testing prior to the implementation or modification of the Information Systems Processing Personal Data do not use real or 'live' data unless such use is necessary and there is no reasonable alternative. Where real or 'live' data is used, it is limited to the extent necessary for the purposes of testing and the level of security corresponding to the type of Personal Data Processed is guaranteed.

3. Audit

a. Regular audits of compliance with these security measures, at least at two yearly intervals, are performed and delivered in the form of an audit report.

b. The audit report provides an opinion on the extent to which the security measures and controls adopted comply with these security measures, identify any shortcomings and (if any) propose corrective or supplementary measures as necessary. It also includes the data, facts and observations on which the opinions reached, and the recommendations proposed are based.

IV. High Security Measures

A. Organizational Measures

1. Security Incident Reporting

a. The procedure for reporting, managing and responding to Security Incidents is tested periodically.

B. Technical Measures

1. Distribution of Media

a. Media containing Personal Data will only be distributed if the data have been encrypted to guarantee that that Personal Data and other information is not intelligible or may not be manipulated in transit.

2. Access Record

a. The minimum details to be recorded for every access to the Information Systems is the User ID, the date and the time of access, the data accessed, the kind of access and whether this was authorized or denied.

b. If access was authorized, the retained information permits to identify the record that was accessed.

c. The mechanisms permitting the data set out in detail in the preceding paragraphs to be recorded are under the direct control of the Security Officer and under no circumstances it is permissible to deactivate these.

d. The minimum period for retaining the data recorded is one year.

e. The Security Officer periodically reviews the control information recorded.

3. Back-Up Copies and Recovery

a. Back-up copies and data recovery procedures are kept at a different location from the site of the Information Systems Processing the Personal Data and these security measures apply to such back-up copies.

4. Electronic Communications Networks

a. Personal Data will be distributed via electronic communications networks only if they have been encrypted, enciphered or another mechanism is used to guarantee that the information is not intelligible or is not manipulated by third parties.

Annex B

Annexes I and II of the EU SCCs

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

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

Name: The exporter is the Customer specified in the Agreement.

Address: As specified in the Agreement.

Contact person's name, position and contact details: As specified in the Agreement.

Activities relevant to the data transferred under these Clauses: Obtaining the Services from Data Importer

Role (controller/processor): Controller

Data importer(s):

Name: AppDirect, Inc.

Address: 650 California Street, Floor 25, San Francisco, CA 94108

Contact person's name, position and contact details: Legal Department, privacy@appdirect.com

Activities relevant to the data transferred under these Clauses: Providing the Services to Data Exporter.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Any individual accessing and/or using the Services through the Company's account; and any individual whose information is stored on or collected via the Services.

Categories of personal data transferred

Identification and contact data (e.g. name, address, title, contact details, username etc.); financial information (e.g. credit card details, account details, payment information etc.); employment details (e.g. employer, job title, geographic location, area of responsibility etc.); order data (e.g. documentation of all orders done incl. all order data e.g. item, product, quantity, price etc.); automatic mail traffic (e.g. with order process or changes in the user structure etc.).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None anticipated.

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

Continuously, for the length of the Agreement between the parties.

Nature of the processing

AppDirect provides the cloud service commerce platform and the support services for the platform. The platform allows Company, its Customers and End Users accessing the platform to purchase and manage subscriptions for Products and any of their End Users to access and use the platform, as described in the Agreement.

Purpose(s) of the data transfer and further processing

The provision of the Services to the Company and the performance of AppDirect's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

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

Until the termination of the Agreement in accordance with its terms.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

AppDirect's subprocessors will process personal data to assist AppDirect in providing the AppDirect services pursuant to the Agreement, for as long as needed for AppDirect to provide the AppDirect services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

The parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Please see Annex A of the DPA, which describes the technical and organisational security measures implemented by AppDirect.