Created February 2023

SMARKETING CLOUD

data compliance and security policy report

The following is a report generated by Cert Pro in partnership with Drata to highlight the policies and procedures that SMARKETING CLOUD LTD carries out to ensure data security, compliance and safeguarding of data in accordance with ISO27001 standards.

Report created 28/02/2023

ISO 27001 is a widely recognized standard for information security management systems (ISMS) and defines a set of policies and procedures that an organisation must follow to ensure the confidentiality, integrity, and availability of its information assets.

Below is an overview of a policy for Continuous Control Monitoring by Smarketing Cloud in accordance with ISO 27001 standards:

1. Purpose: The purpose of this policy is to ensure that Smarketing Cloud's continuous control monitoring process is implemented and maintained in compliance with ISO 27001 and other relevant regulations and standards.

2. Scope: This policy applies to all employees and stakeholders involved in the continuous control monitoring process.

3. Asset Inventory: To ensure effective continuous control monitoring, it is essential to know all physical and virtual assets across the company. Smarketing Cloud's automated inventory system will be used to maintain an up-to-date record of all assets. This inventory will be reviewed regularly and any changes will be recorded in the asset register.

4. Risk Assessment: Smarketing Cloud's built-in self-assessments will be used to assess the effectiveness of the organisation's security program. The results will be analysed to identify areas for improvement and to maintain compliance with ISO 27001 and other relevant regulations and standards.

5. Continuous Control Monitoring: Smarketing Cloud's continuous control monitoring process will be used to detect and respond to security incidents in a timely manner. This process will be continuously reviewed and improved to ensure its effectiveness.

6. Vendor Management: All vendors that support the organisation's security infrastructure, including Subprocessors, will be managed through a centralised location for storing, sending, and reviewing security questionnaires. This will ensure that all vendors meet the organisation's security requirements and are compliant with relevant regulations and standards.

7. Infrastructure Subprocessors: Smarketing Cloud may use the listed Infrastructure Sub Processors to host customer data or provide other infrastructure that helps with delivery of the services. These Subprocessors are audited for security and are located in the EU.

8. Other Subprocessors: Smarketing Cloud may use the listed Other Subprocessors to perform other service functions. These Subprocessors are audited for security and are located in the EU or the United States.

9. Policy Center: Smarketing Cloud's Policy Center will be used to streamline documentation, employee acceptance, and version history with 20+ editable, auditor-approved policies.

10. Updates: Smarketing Cloud will provide notice of any new Subprocessors to the customer account owner, as required under the agreement, and will post such updates on the website. It is the responsibility of all stakeholders to check for updates regularly.

Overall, this policy ensures that Smarketing Cloud's continuous control monitoring process is implemented and maintained effectively, enabling the organisation to stay compliant with ISO 27001 and other relevant regulations and standards, and maintain full visibility into its security status at all times.

Smarketing Cloud understands that the implementation of an ISMS in accordance with ISO/IEC 27001 is critical to maintaining the confidentiality, integrity, and availability of information assets.

By following the 14 points outlined in this policy document, Smarketing Cloud can ensure that its ISMS is comprehensive and effective in protecting the organisation's information assets. Smarketing Cloud will regularly review and update its ISMS to ensure its continued effectiveness and compliance with the ISO/IEC 27001 standard.

Information Security Policies:

Smarketing Cloud understands the importance of information security policies in protecting our organisation's confidentiality, integrity, and availability of information assets. We have established, implemented, maintained, and reviewed information security policies that align with our objectives and requirements. We communicate these policies to all relevant stakeholders, including employees, contractors, and suppliers. We regularly review and update our information security policies to ensure their continued effectiveness and compliance with applicable laws and regulations.

Organization of Information Security:

We organise our information security activities at Smarketing Cloud to ensure that they are effective, efficient, and aligned with our objectives and requirements. We define roles and responsibilities for individuals involved in information security and ensure that they have the necessary knowledge, skills, and resources to perform their duties effectively. We regularly review and update our information security organisation to ensure its continued effectiveness and compliance with applicable laws and regulations.

Asset Management:

Smarketing Cloud manages information assets to ensure that they are protected from unauthorised access, use, disclosure, modification, or destruction. We identify, classify, and assign ownership to information assets, and implement appropriate controls to protect them based on their value and risk. We regularly review and update our asset management processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Human Resources Security:

We recognize that human resources are a critical element of our information security management system at Smarketing Cloud. We manage our human resources to ensure that they are trustworthy and competent and that they have the necessary knowledge, skills, and resources to perform their duties effectively. We implement appropriate controls to ensure that our human resources are aware of their information security responsibilities and comply with applicable laws and regulations. We regularly review and update our human resources security processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Physical and Environmental Security:

Smarketing Cloud protects information assets from physical and environmental threats such as theft, fire, flood, or other disasters. We implement appropriate controls to ensure that our physical and environmental security measures are effective and comply with applicable laws and regulations. We regularly review and update our physical and environmental security processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Communications and Operations Management:

We manage our information and communication technology (ICT) resources at Smarketing Cloud to ensure their availability, integrity, and confidentiality. We implement appropriate controls to ensure that our ICT resources are secure and comply with applicable laws and regulations. We regularly review and update our communications and operations management processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Access Control:

We control access to our information assets at Smarketing Cloud to ensure that only authorised individuals are allowed to access them. We implement appropriate controls to ensure that our access control measures are effective and comply with applicable laws and regulations. We regularly review and update our access control processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Information Systems Acquisition, Development, and Maintenance:

Smarketing Cloud manages the acquisition, development, and maintenance of information systems to ensure that they are secure and comply with applicable laws and regulations. We implement appropriate controls to ensure that our information systems are effective and comply with applicable laws and regulations. We regularly review and update our information systems acquisition, development, and maintenance processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Information Security Incident Management:

We manage information security incidents at Smarketing Cloud to ensure that they are detected, responded to, and recovered from in a timely and effective manner. We have a documented incident management process that defines roles, responsibilities, and procedures for managing incidents. We regularly test and update our incident management process to ensure its continued effectiveness and compliance with applicable laws and regulations.

Business Continuity Management:

Smarketing Cloud manages business continuity in the event of a disruption or disaster. We have a documented business continuity plan that outlines how we will maintain essential business functions during and after a disruption or disaster. We regularly review and update our business continuity plan to ensure its continued effectiveness and compliance with applicable laws and regulations.

Compliance:

We comply with legal, regulatory, and contractual requirements related to information security at Smarketing Cloud. We regularly monitor changes in applicable laws and regulations to ensure that we remain compliant. We implement appropriate controls to ensure that we comply with applicable laws and regulations. We regularly review and update our compliance processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Cryptography:

We use cryptography to protect our information assets at Smarketing Cloud. We implement appropriate controls to ensure that our cryptography measures are effective and comply with applicable laws and regulations. We regularly review and update our cryptography processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Physical Security:

We protect physical infrastructure, including buildings, equipment, and other assets, at Smarketing Cloud. We implement appropriate controls to ensure that our physical security measures are effective and comply with applicable laws and regulations. We regularly review and update our physical security processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Supplier Relationships:

At Smarketing Cloud, we manage relationships with suppliers, including their selection, monitoring, and termination, with respect to information security. We implement appropriate controls to ensure that our suppliers are aware of their information security responsibilities and comply with applicable laws and regulations. We regularly review and update our supplier relationship processes to ensure their continued effectiveness and compliance with applicable laws and regulations.

Statement of intention:

Smarketing Cloud is committed to implementing and maintaining an effective information security management system in compliance with the ISO/IEC 27001 standard. We recognize that the 14 domains of ISO/IEC 27001 are critical for achieving this goal, and we have implemented appropriate policies and processes to ensure their effectiveness and compliance with applicable laws and regulations. We regularly review and update our policies and processes to ensure their continued effectiveness and compliance.

Continuous Monitoring

Infrastructure Security

- Cloud Data Storage Restricted
- Password Policy
- Security Patches Automatically Applied
- Multiple Availability Zones
- Encryption of Web-Based Admin Access

Network Security

- Malware Detection Software
- Logging/Monitoring
- Firewalls
- Denial of Public SSH
- Unique Accounts Used

Data Security

- Security Policy
- System Access Control Policy
- Daily Database Backups
- SSL/TLS Enforced
- Encryption at Rest

Product Security

- Servers Monitored & Alarmed
- NoSQL Database Monitored and Alarmed
- Messaging Queues Monitored & Alarmed
- Databases Monitored & Alarmed
- MFA on Accounts
- Terms of Service
- Hard-Disk Encryption
- Login Password

App Security

- Employee Disclosure Process
- Responsible Disclosure (Bug Bounty)
- Annual Penetration Test
- Quarterly Vulnerability Scan
- Vulnerability Management
- Code Review Process
- Software Development Lifecycle
- Web Application Firewall

Organization Security

- BCDR Plan
- Disaster Recovery Plan
- Incident Response Team
- Incident Response Plan
- Code of Conduct

- Acceptable Use Policy
- Security Training

Infrastructure Sub-processors:

Infrastructure Sub-processors play an important role in hosting customer data or providing other infrastructure that helps with delivery of Smarketing Cloud's services. Therefore, it is crucial to ensure that these Sub-processors comply with all applicable laws, regulations, and standards regarding the protection of personal data. The following policy section outlines the guidelines for the use of Infrastructure

Sub-processors:

1. Purpose: The purpose of this policy section is to ensure that Smarketing Cloud's use of Infrastructure Sub-processors is in compliance with all applicable laws, regulations, and standards regarding the protection of personal data.
2. Data Location: All Infrastructure Sub-processors must be located in the EU, unless an alternative location has been specifically approved by the relevant Data Protection Authority or other regulatory body.
3. Due Diligence: Smarketing Cloud will perform due diligence on all Infrastructure Sub-processors before engaging their services. This includes evaluating their security measures, their compliance with relevant regulations and standards, and their ability to maintain the confidentiality, integrity, and availability of customer data.
4. Contractual Obligations: All Infrastructure Sub-processors must be contractually obligated to comply with Smarketing Cloud's data protection and security policies, as well as all applicable laws, regulations, and standards. These obligations must be clearly outlined in the service contract and must include provisions for regular monitoring and auditing of the Sub-processor's performance.
5. Notification: Smarketing Cloud will notify its customers of any new Infrastructure Sub-processors or changes to existing ones. This notification will include information about the purpose of the Sub-processor, its data location, and any relevant contractual obligations.
6. Termination: Smarketing Cloud reserves the right to terminate its relationship with any Infrastructure Sub-processor that fails to comply with its data protection and security policies, or any applicable laws, regulations, or standards. The termination process will include a review of the Sub-processor's performance and a determination of whether any corrective actions are required.

Overall, the use of Infrastructure Sub-processors is critical to the delivery of Smarketing Cloud's services. Therefore, it is important to ensure that these Sub-processors comply with all applicable laws, regulations, and standards regarding the protection of personal data.

By following the guidelines outlined in this policy section, Smarketing Cloud can ensure that its use of Infrastructure Sub-processors is both effective and compliant with all relevant regulations and standards.

Sub-Processor	Purpose	Data Location
Digital Ocean	Hosting & Infrastructure	EU
Cloudflare, Inc.	Content delivery network & WAF	EU

Other Sub-processors:

Smarketing Cloud may use the following Subprocessors to perform other Service functions:

Sub-Processor	Purpose	Data Location
Amplitude, Inc.	Product Analytics	EU
Functional Software, Inc.	Client-side error tracking for debugging, troubleshooting, auditing, and reporting	EU
Slack Technologies	Cloud-based Team Chat Services	United States
SendGrid	Email Sending	United States

Twilio, Inc.	Segment: Cloud-based CDP tool	United States
Zapier Inc.	Automation Workflow	United States

Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of the agreement between Smarketing Cloud and its Customers ("Agreement"). It sets out the terms and conditions governing the processing of Personal Data by Smarketing Cloud on behalf of the Customer in accordance with applicable data protection laws, including but not limited to the General Data Protection Regulation ("GDPR").

Definitions

For the purpose of this DPA, the following definitions shall apply:

1.1 "Customer" means the organisation that has subscribed to Smarketing Cloud services.

1.2 "Data Protection Laws" means all laws and regulations applicable to the processing of Personal Data under this DPA, including the GDPR.

1.3 "Personal Data" means any information relating to an identified or identifiable natural person.

1.4 "Processor" means the party that processes Personal Data on behalf of the Customer.

1.5 "Sub-processor" means any third-party Processor engaged by Smarketing Cloud to process Personal Data on behalf of the Customer.

Purpose and Scope

2.1 This DPA sets out the terms and conditions governing the processing of Personal Data by Smarketing Cloud on behalf of the Customer under the Agreement.

2.2 Smarketing Cloud shall process Personal Data only for the purpose of providing the services under the Agreement.

2.3 The Customer acknowledges that it is the data controller and Smarketing Cloud is the data processor.

Obligations of Smarketing Cloud

3.1 Smarketing Cloud shall process Personal Data only in accordance with the instructions of the Customer, unless required to do otherwise by applicable law.

3.2 Smarketing Cloud shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing of

Personal Data.

3.3 Smarketing Cloud shall ensure that its personnel involved in the processing of Personal Data are bound by confidentiality obligations.

3.4 Smarketing Cloud shall assist the Customer in complying with its obligations under Data Protection Laws, including but not limited to the GDPR, to the extent necessary for the performance of the services under the Agreement.

3.5 Smarketing Cloud shall notify the Customer without undue delay after becoming aware of any Personal Data breach.

3.6 Smarketing Cloud shall not engage any Sub-processor without the prior written consent of the Customer.

3.7 Smarketing Cloud shall ensure that any Sub-processor engaged by it to process Personal Data on behalf of the Customer is bound by obligations equivalent to those set out in this DPA.

Obligations of the Customer

4.1 The Customer shall provide instructions to Smarketing Cloud for the processing of Personal Data.

4.2 The Customer shall ensure that it has obtained all necessary consents, authorizations, and permissions required under Data Protection Laws to enable Smarketing Cloud to process Personal Data in accordance with the Agreement.

4.3 The Customer shall comply with its obligations under Data Protection Laws, including but not limited to the GDPR.

4.4 The Customer shall notify Smarketing Cloud without undue delay after becoming aware of any Personal Data breach.

Data Subject Rights

5.1 Smarketing Cloud shall, to the extent possible, assist the Customer in responding to requests from data subjects to exercise their rights under Data Protection Laws.

5.2 Smarketing Cloud shall provide reasonable assistance to the Customer in fulfilling its obligations under Data Protection Laws to the extent necessary for the performance of the services under the Agreement.

Termination and Deletion

6.1 Upon termination of the Agreement, Smarketing Cloud shall delete or return all Personal Data to the Customer, unless required by applicable law to retain it.

6.2 Smarketing Cloud shall ensure that any Sub-processor engaged by it to process Personal Data on behalf of the Customer shall also delete or return all Personal Data to the Customer upon request.

SCHEDULE 1

TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

For the purposes of the EU C-to-P Transfer Clauses and the EU P-to-P Transfer Clauses, Customer is the data exporter and Smarketing Cloud is the data importer and the parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses or the EU P-to-P Transfer Clauses for the transfer of Personal Data, any references to 'Customer' in this Schedule include such Authorised Affiliate. Where this Schedule 1 does not explicitly mention EU C-to-P Transfer Clauses or EU P-to-P Transfer Clauses it applies to both of them.

STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

1.1. **Reference to the Standard Contractual Clauses**. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.
1.2. **Docking clause**. The option under clause 7 shall not apply.
1.3. **Instructions**. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Smarketing Cloud for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

1.4. **Certification of Deletion**. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Smarketing Cloud to Customer only upon Customer's written request.

1.5. **Audits of the SCCs**. The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 4.3 of this DPA.

1.6. **General authorization for use of Subprocessors**. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Smarketing Cloud has Customer's general authorization to engage Subprocessors in accordance with section 7 of this DPA. Smarketing Cloud shall make available to Customer the current list of Sub Processors in accordance with section 7 of this DPA. Where Smarketing Cloud enters into the EU P-to-P Transfer Clauses with a Subprocessor in connection with the provision of the Services, Customer hereby grants Smarketing Cloud and Smarketing Cloud's Affiliates authority to provide a general authorization on Controller's behalf for the engagement of sub processors by Subprocessors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such subprocessors.

1.7. **Notification of New Subprocessors and Objection Right for new Subprocessors**. Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Smarketing Cloud may engage new Subprocessors as described in section 7 of this DPA. Smarketing Cloud shall inform Customer of any changes to Subprocessors following the procedure provided for in section 7 of this DPA.

1.8. **Complaints - Redress**. Smarketing Cloud shall inform Customer if it receives a Data Subject Request with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Smarketing Cloud shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

1.9. **Liability**. Smarketing Cloud's liability under clause 12(b) shall be limited to any damage caused by its Processing where Smarketing Cloud has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.

1.10. **Supervision**. Clause 13 shall apply as follows:

1.10.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

1.10.2. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

1.10.3. Where Customer is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as competent supervisory authority.

1.10.4. Where Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws.

1.11. **Notification of Government Access Requests**. For the purposes of clause 15(1)(a), Smarketing Cloud shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customers shall be solely responsible for promptly notifying the Data Subject as necessary.

1.12. **Governing Law**. The governing law for the purposes of clause 17 shall be the law that is designated in the section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

1.13. **Choice of forum and jurisdiction**. The courts under clause 18 shall be those designated in the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

1.14. Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses. In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Applicable Data Protection Laws of the United Kingdom ("UK Data Protection Laws") or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

1. 1.15. **Conflict.** The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

ADDITIONAL TERMS FOR THE EU P-TO-P TRANSFER CLAUSES

For the purposes of the EU P-to-P Transfer Clauses (only), the parties agree the following.

2.1. Instructions and notifications. For the purposes 8.1(a), Customer hereby informs Smarketing Cloud that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Smarketing Cloud for the appointment of Subprocessors in accordance with this DPA, have been authorised by the relevant Controller. Customers shall be solely responsible for forwarding any notifications received from Smarketing Cloud to the relevant Controller where appropriate.
2.2. Security of Processing. For the purposes of clause 8.6(c) and (d), Smarketing Cloud shall provide notification of a personal data breach concerning Personal Data Processed by Smarketing Cloud to Customer.

2.3. Documentation and Compliance. For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Smarketing Cloud by Customer. If Smarketing Cloud receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

2. 2.4. Data Subject Rights. For the purposes of clause 10 and subject to section 3 of this DPA, Smarketing Cloud shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customers shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

SCHEDULE 2

DESCRIPTION OF PERSONAL DATA PROCESSING

This Schedule forms part of the Standard Contractual Clauses and must be completed and signed by the parties. As evidenced by the signature of each party's authorised representative below, the data Processing activities carried out by Smarketing Cloud under the Agreement may be described as follows:

1. Subject Matter
   . The parties acknowledge and agree that the subject matter of the Processing is data importer's provision of the Services to data exporter as fully described in this DPA and/or the Agreement.
2. Duration
   . The duration of the Processing of Customer Personal Data is for the Term or until the disposal of all Personal Data, whichever is later.
3. Nature and Purpose
   . The nature and purpose of the Processing of Personal Data is for data importer's provision of the Services to data exporter.
4. Data Categories
   . Categories of personal data are identification and contact data (for example, name, address, title, contact details), employment details (for example, employer, job title, geographic location and area of responsibility), and IT information (for example, IP addresses, usage data, cookies data, device specific information, connection data and location data) of the data subjects.
5. Special Data Categories
   . Data exporter is prohibited from providing data importer with sensitive personal information (such as financial, medical or other sensitive personal information such as government IDs, passport numbers or

social security numbers), and data importer has no obligation to comply with the DPA with respect to such data.

6. Data Subjects
   . The employees of a data exporter.

SCHEDULE 3

CALIFORNIA SCHEDULE

1. For purposes of this Schedule 2, the terms “business,” “commercial purpose,” “sell” and “service provider” shall have the respective meanings given thereto in the CCPA, and “personal information” shall mean Personal Data that constitutes personal information, the Processing of which is governed by the CCPA.
2. It is the parties’ intent that with respect to any personal information, Smarketing Cloud is a service provider. Smarketing Cloud shall (i) not “sell” (as defined in the CCPA) personal information; and (ii) not retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using or disclosing personal information for a commercial purpose (as defined in the CCPA) other than providing the Services. For the avoidance of doubt, the foregoing prohibits Smarketing Cloud from retaining, using or disclosing personal information outside of the direct business relationship between Smarketing Cloud and Customer. Smarketing Cloud hereby certifies that it understands the obligations under this section 2 and shall comply with them.
3. The parties acknowledge that Smarketing Cloud’s retention, use and disclosure of personal information authorised by Customer’s instructions documented in the DPA are integral to Smarketing Cloud’s provision of the Services and the business relationship between the parties.

SCHEDULE 4

Security Measures

1. Organisational management and dedicated staff responsible for the development, implementation and maintenance of the Smarketing Cloud’s information security program.
2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Smarketing Cloud’s organisation, monitoring and maintaining compliance with the Smarketing Cloud’s policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
3. Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available industry-standard encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly

or at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).
5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that the Smarketing Cloud's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on the Smarketing Cloud's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.
6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.
7. Physical and environmental security of data centres, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorised physical access, (ii) manage, monitor and log movement of persons into and out of the Smarketing Cloud's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Smarketing Cloud's possession.
9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the Smarketing Cloud's technology and information assets.
10. Incident management procedures designed to allow Smarketing Cloud to investigate, respond to, mitigate and notify of events related to the Smarketing Cloud's technology and information assets.
11. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
12. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.

Contact your representative for additional documents

- Software Development Life Cycle Policy

- Disaster Recovery Plan
- Information Security Policy
- Risk Assessment Policy
- Vendor Management Policy
- Business Continuity Plan
- Incident Response Plan
- Vulnerability Management Policy
- Smarketing Cloud Vendor Security Questionnaire

Updates

As our business grows and evolves, the Sub-processors we engage in may also change. We will endeavour to provide the owner of Customer's account with notice of any new Subprocessors to the extent required under the Agreement, along with posting such updates here.

Please check back frequently for updates.