MOBILEIRON, INC.
Data Protection Schedule
(version May 15, 2018)

This Data Protection Schedule, including the Exhibits (collectively, the "**DPA**"), supplements and is incorporated in and forms a part of a Customer Agreement made by and between Customer and MobileIron (the "**Agreement**"). In the event of a conflict between a provision of this DPA and a provision of the Agreement, the DPA will control with respect to its terms.

1. Definitions.

a. Capitalized terms used and not defined in this DPA have the meaning given them in the Agreement.

b. "**Customer Data**" means all Personal Data provided to MobileIron by or on behalf of Customer through use of Online Services, the extent of which is determined by Customer in its sole discretion.

c. "**Documentation**" means the written and/or electronic release notes, implementation guides, or other published technical documentation about a MobileIron Solution that is provided or made available to Customer by MobileIron.

d. "**End User**" means an individual who uses a MobileIron Solution.

e. "**MobileIron Solution**" means either of the SaaS Product or Software, or both the SaaS Product and Software.

f. "**Online Services**" means MobileIron-hosted services that Customer purchases under the Agreement as standalone services or as included with a MobileIron platform or application. Online Services do not include MobileIron Government Cloud, free trials, any separately-branded service that operates outside of MobileIron's control, or software and services provided under separate license or subscription terms. Online Services do not include Software, but may include any MobileIron-hosted service that is necessary for the full functioning of Software.

g. "**Order**" means any purchase order, product schedule or ordering document between Customer and an authorized reseller or, if purchasing directly from MobileIron, between Customer and MobileIron, that identifies the MobileIron Solution and/or services licensed or sold and any applicable subscription or licensing parameters (e.g., the number of subscriptions).

h. "**Personal Data**" means any information submitted to Online Services and relating to (i) an identified or identifiable natural person and (ii) an identified or identifiable legal entity where such information is protected similarly as Personal Data or personally identifiable information under applicable data protection laws. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

i. "**SaaS Product**" means the services made available by access to and use of software hosted by or for MobileIron, including any Documentation.

j. "**Security Incident**" means any unlawful access to any Personal Data stored on MobileIron's equipment or in MobileIron's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Personal Data.

k. "**Software**" means the object code version of MobileIron proprietary computer programs made available by MobileIron for download by Customer (including for use in connection with any SaaS Product), including any Documentation and Updates.

l. "**Subprocessors**" means the other processors that are used by MobileIron to process Personal Data on behalf of Customer. For avoidance of doubt, MobileIron's colocation data center facilities are not Subprocessors.

m. "**Support Data**" means all Personal Data, other than Customer Data, provided to MobileIron by or on behalf of Customer (or that Customer authorizes MobileIron to obtain from Online Services) through an engagement with MobileIron to obtain technical support and/or consulting services for Online Services or Software covered under the Agreement, the extent of which is controlled by Customer in its sole discretion.

n. "**Term**" means the term of the SaaS Product subscription or Software license, as identified in the relevant Order, starting when MobileIron first makes available the credentials to access and use the SaaS Product, or the Software for download.

o. "**Updates**" means any correction, update, upgrade, patch, or other modification or addition made by MobileIron to specific Software.

2. Compliance With Laws.

a. MobileIron. MobileIron must comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. All Security Incidents are subject to Section 7. MobileIron is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. MobileIron does not determine whether Customer Data or Support Data include information subject to any specific law or regulation.

b. Customer. Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to privacy, Personal Data, biometric data, data protection and confidentiality of communications. Customer is responsible

for (i) implementing and maintaining privacy protections and security measures for components and MobileIron Solution configurations that Customer provides or controls (including devices enrolled with a MobileIron Solution), (ii) determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation, (iii) using the Online Services consistently with Customer's legal and regulatory obligations, (iv) making disclosures, obtaining consents, and providing access, choices and other applicable rights to end users with regard to the processing of Personal Data that are required under applicable law, rules or regulations, and (v) responding to any request from a third party regarding Customer's use of Online Services. For clarity, Customer may influence the scope and the manner of the processing of its Personal Data by its own implementation, configuration and use of the Online Services, including any other products or services offer by MobileIron and third-party integrations.

3. Use of Data.

a. Customer Data and Support Data. Customer Data will be used only to provide Customer the Online Services (including compatible purposes) such as to implement and deliver the MobileIron Solution and its features and associated services, provide Customer support, and help Customer prevent or address service or technical problems. Support Data will be used only to provide Customer with support (including compatible purposes), such as troubleshooting recurring issues and improvements to support or to the Online Services. MobileIron will not use either Customer Data or Support Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data and Support Data. MobileIron acquires no rights in Customer Data or Support Data, other than the rights Customer grants to MobileIron to provide the Online Services to Customer or to provide support to Customer. This paragraph does not affect MobileIron's rights in MobileIron Solutions purchased by Customer.

b. Aggregated, De-Identified Data. MobileIron collects, analyzes, and uses aggregated, anonymized or de-identified data and related information (such as product or feature usage, device metrics/metadata and/or mobile application usage) as permitted under applicable law to facilitate market research, product development/improvement, product utilization analyses and support and maintenance services. MobileIron may use, store, or disclose such data or material derived from such information, if it does not identify or is not attributable to any individual.

4. **Professional Services and Related Data**. Professional services are not Online Services, and information provided to MobileIron during a professional services engagement is protected under the confidentiality terms of the Agreement. The rest of this DPA does not apply to such information, unless it is Personal Data subject to Section 14 of this DPA.

5. Non-Disclosure of Data

a. MobileIron will not disclose Customer Data or Support Data outside of MobileIron or its controlled subsidiaries and affiliates except (i) as Customer directs, (ii) as described in the Agreement, or (iii) as required by law.

b. Upon receipt of any third-party request or demand for Customer Data or Support Data, MobileIron will promptly notify Customer except as prohibited by law. MobileIron will reject the request unless required by law to comply. If the request is valid, MobileIron will attempt to redirect the third party to make the request or demand directly to Customer.

c. MobileIron will not provide to any third party: (i) direct, indirect, blanket or unfettered access to Customer Data or Support Data; (ii) encryption keys used to secure Customer Data or Support Data or the ability to break such encryption; or (iii) access to Customer Data or Support Data if MobileIron is aware that the data is to be used for purposes other than those stated in the third party's request.

6. **Security.** MobileIron is committed to helping protect the security of Customer Data. MobileIron has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. In that regard, MobileIron has implemented and will maintain and follow for the computer systems that host or communicate with Online Services the security measures described in the following table which, in conjunction with any security commitments in the Agreement and without prejudice to Customer's obligations under Section 2.b, are MobileIron's only responsibility with respect to the security of Customer Data. MobileIron may update or modify the security measures described below time to time if such update or modification does not result in the degradation of overall security.

Security Control Category	Description
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing MobileIron's administrative, physical, and technical safeguards designed to protect the security, confidentiality and integrity of Personal Data b. Use of security personnel that are sufficiently trained, qualified and experienced to be able to fulfill their information security-related functions
2. Access Controls	a. Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Data, relevant systems and the organization's premises b. Maintain controls designed to limit access to Personal Data, relevant systems and the facilities hosting the systems to authorized personnel c. Review personnel access rights on a regular and periodic basis d. Maintain physical access controls to facilities containing systems, including by using access cards or fobs issued to MobileIron personnel as appropriate e. Maintain policies requiring termination of physical and electronic access to Personal Data and systems after termination of an employee f. Access controls designed to authenticate users and limit access to systems g. Policies restricting access to the data center facilities hosting systems to approved data center personnel and limited and approved MobileIron personnel. h. Maintain dual layer access authentication processes for MobileIron employees with administrative access rights to systems
3. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur c. Documentation of formal risk assessments d. Review of formal risk assessments by appropriate managerial personnel
4. Data Classification, Retention and Deletion	a. Maintain policies establishing data classification based on data criticality and sensitivity. b. Maintain policies establishing data retention and secure destruction requirements
5. Personnel Background Checks	Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Data or relevant systems, subject to local law
6. Personnel Training and Education	Regularly and periodically train personnel, on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
7. Vendor Management and Oversight	Periodically review available security assessment reports of vendors hosting the systems to assess their security controls and analyze any exceptions set forth in such reports
8. Monitoring, Intrusion Detection and Incident Response	a. Monitor the access, availability, capacity and performance of the systems, and related firewalls, system logs and server traffic using various monitoring software and services b. Maintain Intrusion detection/prevention (IDS/IPS) on systems located in the United States and directly accessible through a load balancer c. Maintain incident response procedures for identifying, reporting and acting on security incidents d. Establish a cross-disciplinary security incident response team
9. Encryption	a. Encryption of Personal Data over HTTPS using SSL when transmitted by web-based applications, and minimum 128-bit encryption for all such traffic b. Production data is encrypted and backed up to the offsite location
10. Firewalls	Maintain hardware and software firewalls to protect systems
11. Change Controls	a. Assign responsibility for system security, system changes and maintenance b. Test, evaluate and authorize major system components prior to implementation
12. Physical Security	Use of colocation facilities and managed data centers hosting the systems that employ: a. multiple levels of physical security, including 24x365 interior and exterior surveillance, and access logging b. uninterruptable power supplies (UPS), generators and cooling systems
13. System Administration and Availability	a. Use of Border Gateway Protocol (BGP) with at least two top-tier ISPs designed to maintain Internet access at data center facilities hosting the systems b. Maintain security patching processes for systems that document current patch levels, determine availability of patches, and establish processes for testing and implementing patches

7. **Security Incident Notification**

a. If MobileIron becomes aware of a Security Incident, MobileIron will promptly (i) notify Customer of the Security Incident; (ii) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. MobileIron will assign and train personnel to (i) liaise with Customer regarding any Personal Data security issues; (ii) receive notice of any Security Incident; (iii) provide notice of any such Security Incident to Customer in accordance with this Section 7 and applicable

law; and (iv) coordinate MobileIron's Security Incident response and remedial action. MobileIron's obligation to notify or respond is not an acknowledgement by MobileIron of any fault or liability with respect to the Security Incident.

b. Customer must (i) ensure Customer's administrators maintain accurate contact information for each MobileIron Solution and (ii) notify MobileIron promptly about any possible misuse of its accounts or authentication credentials or any Security Incident related to Online Services.

8. **Location of Data Processing**. Except as described elsewhere in the Agreement, Customer Data and Support Data that MobileIron processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which MobileIron or its affiliates or subcontractors maintain facilities. Generally, MobileIron will store Customer Data within the available region that is either (i) selected by Customer (if available for the Online Services) or (ii) determined based on contact information provided by Customer. If Customer decides, in Customer's sole discretion, to submit Customer Data and Support Data to MobileIron with a request for technical support, MobileIron may store limited Customer Data and Support Data in other locations to provide support as directed by Customer. Customer appoints MobileIron to perform any such transfer of Customer Data and Support Data to any such country and to store and process Customer Data and Support Data to provide the Online Services.

9. **Data Retention**. At all times during the Term for standalone Online Services, Customer will have the ability to access and extract Customer Data stored in the Online Services, where feasible. Except for free trials, MobileIron will retain Customer Data stored in standalone Online Services for at least 90 days after expiration of the Term or the related subscription or license so that Customer may extract the data. After the 90-day retention period, MobileIron will disable Customer's account and delete the Customer Data.

10. **MobileIron Personnel**. MobileIron personnel will not process Customer Data or Support Data without authorization from Customer. MobileIron personnel are obligated to maintain the confidentiality of Customer Data and Support Data as provided in this DPA and this obligation continues even after their engagements end.

11. **Subcontractors.** MobileIron may engage subcontractors, including MobileIron's corporate affiliates, for limited or ancillary services on its behalf. Any such subcontractors will be permitted to obtain Customer Data and Support Data only to deliver the services MobileIron has retained them to provide and will be prohibited from using Customer Data and Support Data for any other purpose. MobileIron remains responsible for its subcontractors' compliance with MobileIron's obligations in the Agreement. Sections 18 and 19 contain additional terms related to Subprocessors.

12. **Audits and Security Reviews of Online Services**

a. Audits. For standalone Online Services, at least annually MobileIron will initiate an audit of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data by a qualified, independent, third party at MobileIron's selection and expense. Each audit will result in the generation of an audit report ("**Audit Report**"), which will be MobileIron's Confidential Information. The Audit Report will clearly disclose any material findings by the auditor. MobileIron will make good faith, commercially reasonable efforts to remediate (i) issues raised in any Audit Report that reasonably could be expected to have an adverse impact on MobileIron's ability to meet its obligations under Section 6 of this DPA and (ii) material control deficiencies. If Customer requests, MobileIron will provide Customer with the Audit Report or a summary designed to be shared with third parties so that Customer can verify MobileIron's compliance with the security obligations under the DPA. The Audit Report will be subject to non-disclosure and distribution limitations of MobileIron and the auditor.

b. Security Reviews. With reasonable prior notice, annually unless otherwise required by law, MobileIron will make personnel reasonably available to Customer to discuss MobileIron's manner of compliance with Section 6 of this DPA, or will provide Customer with access to information or documentation about MobileIron's information security practices as they relate to this DPA, including without limitation access to any security assessment reports designed to be shared with third parties. Any such information and documentation must be considered MobileIron's Confidential Information.

13. **Additional Australian Terms**. This Section 13 applies only if Customer has end users in Australia. Personal Data is collected, stored, used and/or processed in compliance with the Australian Privacy Act 1988 (Commonwealth) and the Australian Privacy Principles. If Customer becomes dissatisfied with MobileIron's handling of a complaint or does not agree with the resolution proposed by MobileIron, Customer may make a complaint to the Office of the Australian Information Commissioner (OAIC) by contacting the OAIC using the methods listed on their website, https://www.oaic.gov.au/. Alternatively, Customer may request that MobileIron pass on the details of Customer's complaint to the OAIC directly.

14. **Additional European Terms**. Sections 14-19 of this DPA ("**Additional European Terms**") apply to the processing of Personal Data of End Users in the European Economic Area ("**EEA**") or Switzerland by MobileIron on behalf of Customer. Article 28(1) of the European Union General Data Protection Regulation ("**GDPR**") requires an agreement between a controller and processor, and between a processor and subprocessor, that processing be conducted in accordance with technical and organizational measures that meet the requirements of the GDPR and ensure the protection of the rights of data subjects. The Additional European Terms are intended to satisfy that requirement for the parties, including to the extent MobileIron is a processor or subprocessor of Personal Data submitted by Customer through a Professional Services engagement. Terms used but not defined in the Additional European Terms, such as "**personal data breach**", "**processing**", "**controller**", "**processor**", and "**data subject**", will have the meaning given to them in Article 4 of the GDPR.

15. **Intent of the Parties**. The terms in the Agreement, including the Additional European Terms and the other provisions of the DPA, constitute a data processing agreement. For the Online Services, MobileIron is a data processor (or sub-processor) acting on Customer's behalf. As data processor (or sub-processor), MobileIron will only act upon Customer's instructions. The Agreement and the DPA (including the terms and conditions incorporated by reference in either), along with Customer's use and configuration of features in the Online Services, are Customer's complete and final instructions to MobileIron for the processing of Customer Data. Any additional or alternate instructions must be agreed to in writing.

16. **Description of Data Processing**

a. Subject matter and duration. The subject matter of the processing of Personal Data is the performance of Online Services including compatible services. The duration of data processing is for the Term.

b. Nature and purpose. The nature and purpose of the processing shall be to provide the Online Services such as to implement and deliver the MobileIron Solution and its features and associated services, provide Customer support, help Customer prevent or address service or technical problems, and provide Customer with support, such as troubleshooting recurring issues and improvements to support or to the Online Services.

c. Data exporter. Customer is a controller or processor of Personal Data and the data exporter.

d. Data importer. MobileIron, Inc. is a processor or subprocessor of Personal Data and the data importer.

e. Data subjects. The categories of Data Subject to whom the Personal Data relates are Customer's representatives and End Users, generally Customer's personnel who provide MobileIron with their Personal Data by using a MobileIron Solution.

f. Categories of data. The types of Personal Data processed, which varies by MobileIron Solution and Customer use case, may include: (i) basic contact information of End Users for administration of local accounts and to enable electronic communications relating to access control or the management of mobile devices; (ii) basic information about mobile devices to facilitate their registration and the deployment, operation and maintenance of MobileIron Solutions; (iii) names, email addresses, usernames and other Personal Data contained in authentication tokens and Single Sign On certificates about End Users' authentication requests and responses to those requests, to support secure authentication; and (iv) other data in an electronic form used by MobileIron in the context of the MobileIron Solution or submitted by Customer through a Professional Services engagement.

g. Processing operations. The Personal Data transferred will be subject to the following basic processing activities: collect, store, retrieve, consult, use, erase or destruct, disclose by transmission, disseminate or otherwise make available data exporter's data as necessary provide MobileIron Solution in accordance with the data exporter's instructions, including related internal purposes (such as quality control, troubleshooting, product development, etc.).

h. Obligations and rights of Customer. The obligations and rights of Customer are set out in the Agreement and the DPA.

17. **Transfer of Customer Data and Support Data**

a. All transfers of Customer Data and Support Data out of the European Economic Area and Switzerland to countries that do not ensure an adequate level of data protection within the meaning of applicable data protection laws shall be governed by one of the following transfer mechanisms, in the specified order of precedence: First, MobileIron's EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications for transfers to the United States, or second, the model clauses for the transfer of Personal Data to Processors established in third countries approved by the European Commission from time to time, the approved version of which in force at present is set out in the European Commission's Decision 2010/87/EU of 5 February 2010 and in Exhibit A to the Additional European Terms (the "**Standard Contractual Clauses**"). The Standard Contractual Clauses shall be governed by the law of the Member State in which Customer is established.

b. MobileIron will abide by the requirements of applicable data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland. MobileIron agrees to notify Customer if it determines that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

c. Execution of the Agreement by both parties includes execution of the Standard Contractual Clauses. The Standard Contractual Clauses cannot be relied upon to legitimize export of data from any country requiring regulatory approval unless Customer has obtained such regulatory approval.

d. If the Standard Contractual Clauses apply, then (i) Customer agrees to exercise its audit right by instructing MobileIron to execute the audit and review as described in Section 12, (ii) if Customer desires to change this instruction, then Customer has the right to do so as stated in the Standard Contractual Clauses, as requested in writing, and (iii) nothing in this section varies or modifies the Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

18. **GDPR Terms**. MobileIron makes the commitments in Sections 18 and 19 effective on the later of the start of enforcement of the GDPR or Customer's use of Online Services or MobileIron's provision of Professional Services. Section 18 reproduces, with minor edits for clarity, the relevant contractual terms required of processors and controllers by Articles 28, 32 and 33 of the GDPR. Article references are shown in brackets.

a. MobileIron shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, MobileIron shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. [28(2)]

b. MobileIron shall process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by European Union or Member State law to which MobileIron is subject; in such a case, MobileIron shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. [28(3)]

c. MobileIron shall ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. [28(3)]

d. MobileIron shall take all measures required pursuant to Article 32 of the GDPR. [28(3)]

e. MobileIron shall respect the conditions referred to in Section 18.a and 18.k for engaging another processor.

f. MobileIron shall taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR. [28(3)]

g. MobileIron shall assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to MobileIron. [28(3)]

h. MobileIron shall, at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless European Union or Member State law requires storage of the Personal Data. [28(3)]

i. MobileIron shall make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer. [28(3)]

j. MobileIron shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other European Union or Member State data protection provisions. [28(3)]

k. Where MobileIron engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in GDPR Article 28(3) (and reproduced in Section 18.b-19.j) shall be imposed on that other processor by way of a contract or other legal act under European Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, MobileIron shall remain fully liable to the Customer for the performance of that other processor's obligations. [28(4)]

l. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and MobileIron shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. [32(1)]

m. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. [32(2)]

n. Customer and MobileIron shall take steps to ensure that any natural person acting under the authority of Customer or MobileIron who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by European Union or Member State law. [32(4)]

o. MobileIron shall notify Customer without undue delay after becoming aware of a personal data breach. [33(2)] Such notice will, at a minimum, (i) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) communicate the name and contact details of the data protection officer or other contact where more information can be obtained; (iii) describe the likely consequences of the personal data breach; and (iv) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. [33(3)]

19. **Additional GDPR Terms**. This Section 19 provides more details on what Customer can expect from MobileIron to fulfill the terms in Section 18, as well as MobileIron's commitments regarding Articles 34-36 of the GDPR not covered elsewhere in the Agreement.

a. Subprocessors. Customer consents to MobileIron engaging Subprocessors for the processing of Personal Data in accordance with Section 18.a and 18.k. A list of MobileIron's current Subprocessors is available upon request or on MobileIron's website. At least 14 days before authorizing any new Subprocessor to access Personal Data, MobileIron will update the list. Where MobileIron is a processor (and not a subprocessor), the following terms apply: (i) If Customer does not approve of a new Subprocessor, then Customer may terminate any subscription for the affected Online Services without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval; (ii) if the affected Online Services are part of a bundle (or similar single purchase of multiple services), then any termination will apply to the entire bundle; and (iii) as Customer's sole and exclusive remedy, MobileIron will refund to Customer any unused prepaid subscription fees.

b. Data Subject Requests. MobileIron will make available to Customer the Personal Data of its data subjects and the ability to fulfill data subject requests to exercise one or more of their rights under the GDPR in a manner consistent with the functionality of the Online Services and MobileIron's role as a processor. MobileIron shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request if Customer is unable to respond using the functionality of the Online Services. If MobileIron receives a request from Customer's data subject to exercise one or more of its rights under the GDPR, MobileIron will redirect the data subject to make its request directly to Customer.

c. Security Reviews, Audits and Inspections. The Audit Report and other information and documentation described in Section 12 are intended to provide evidence of MobileIron's compliance with the technical and organizational measures that protect the Online Services for purposes of Section 18.i. Upon Customer's written request, MobileIron will make a summary of the data processing terms in its agreements with Subprocessors available to Customer. Customer may request in writing reasonable additional information with respect to a Subprocessor's ability to perform the relevant processing activities in accordance with this DPA.

d. Data Protection Impact Assessments. MobileIron will, on request, provide Customer with reasonable information required to fulfill Customer's obligations to carry out data protection impact assessments, if any, in satisfaction of its obligation under Section 18.g.

20. **Assistance**. Customer must make a written request for any assistance referred to in this DPA. MobileIron may charge Customer no more than a reasonable charge to perform such assistance, to be stated in a quote and agreed by the parties.

MOBILEIRON, INC.
Additional European Terms
Exhibit A: Standard Contractual Clauses (Processors)
(version May 15, 2018)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer

(the "data exporter")

and

MobileIron, Inc.

401 East Middlefield Road, Mountain View, CA 94043, USA **(the "data importer")**

each a "**party**"; together "**the parties**",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause 3, Clause 4(b)-(i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause 3.2, Clause 5(a) to (e) and (g), Clause6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause 3.3, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and

Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do

so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 1 forms part of the Clauses and must be completed by the parties

Data exporter: Customer is the data exporter.

Data importer: MobileIron, Inc. is the data importer.

Data subjects: See Section 16 of the DPA.

Categories of data: See Section 16 of the DPA.

Processing operations: See Section 16 of the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 2 forms part of the Clauses and must be completed by the parties

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached): As described in Section 6 of the DPA.