

Brightfin DPA 3.22.21

DATA PROCESSING AGREEMENT

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“DPA”) is entered into by and between Mobile Solutions Services Holdings, LLC, d/b/a Brightfin, a Delaware corporation with its principal place of business at 10731 E. Easter Ave, Suite #105, Centennial, CO 80112 on behalf of itself and its Affiliates (collectively “Brightfin”) and the business entity identified below (“Customer”) and supplements, with respect to Brightfin’s Processing of Personal Data, the Master Ordering Agreement in effect between Brightfin and Customer under which Brightfin is providing the Subscription Service to Customer (“Agreement”). Any term not defined herein shall have the meaning ascribed to it in the Agreement.

A. INSTRUCTIONS FOR EXECUTING THIS DPA

1. This DPA consists of two parts: (i) the main body of the DPA (Sections 1 to 11); and (ii) the Data Security Guide which is attached hereto and incorporated herein.
2. This DPA has been pre-signed on behalf of Brightfin.
3. To fully execute this DPA, the Customer must:
 - a. Complete the information in the signature box and execute; and
 - b. Submit a completed and fully executed DPA without changes to the printed terms to Brightfin via privacy@brightfin.com.
4. Upon receipt by Brightfin of a fully completed and duly executed DPA, this DPA shall become legally binding.

B. APPLICATION OF THIS DPA

1. If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement and the Brightfin entity that is party to the Agreement is party to this DPA.
2. If the entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA, and, to the extent applicable, Affiliates of such Customer will benefit under this DPA.
3. This DPA shall not diminish nor supersede any additional rights relating to Processing of Customer Data previously negotiated by Customer in the Agreement. In the event of any conflict between the terms of this DPA and the Agreement with respect to the Processing of Personal Data, the DPA shall control.

1. DEFINITIONS

1.1. AFFILIATE. The term “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control by Customer or Brightfin, as applicable.

1.2. DATA CONTROLLER. The term “**Data Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates either permitted by Customer to submit Personal Data to the Subscription Service or whose Personal Data is Processed in the Subscription Service.

1.1. DATA PROCESSOR. The term “**Data Processor**” means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is Brightfin.

1.3. DATA PROTECTION LAWS. The term “**Data Protection Laws**” means all applicable laws and regulations regarding the Processing of Personal Data.

1.2. DATA SUBJECT. The term “**Data Subject**” means an identified or identifiable natural person.

1.3. PERSONAL DATA. The term “**Personal Data**” means any information relating to a Data Subject uploaded by or for Customer or Customer’s agents, employees, or contractors to the Subscription Service as Customer Data.

1.4. PROCESS. The term “**Process**” or “**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.5. SERVICENOW. The term “**ServiceNow**” means collectively ServiceNow, Inc. (USA), and ServiceNow Nederland B.V. (the Netherlands).

1.6. SUB-PROCESSOR. The term “**Sub-Processor**” means any legal person or entity engaged in the Processing of Personal Data by Data Processor.

2. SCOPE OF THE PROCESSING

2.1. COMMISSIONED PROCESSOR. Data Controller appoints Data Processor to Process Personal Data on behalf of Data Controller to the extent necessary to provide the Subscription Service described in the Agreement and in accordance with the Instructions (as defined below).

2.2. INSTRUCTIONS. The Agreement constitutes Data Controller’s written instructions to Data Processor for Processing of Personal Data. Data Controller may issue additional or alternate data processing instructions provided that such instructions are: (a) consistent with the purpose and the scope of the Agreement; and (b) confirmed in writing by Data Controller. For the avoidance of doubt, Data Controller shall not use additional or alternate instructions to alter the scope of the Agreement. For the purposes of this

Agreement, the term “Instructions” means Data Controller’s documented data processing instructions issued to Data Processor in compliance with this Section 2. Data Controller is responsible for ensuring its Instructions to Data Processor comply with Data Protection Laws.

2.3. NATURE, SCOPE AND PURPOSE OF THE PROCESSING. Data Processor shall only Process Personal Data in accordance with Data Controller’s Instructions and to the extent necessary for providing the Subscription Service as described in the Agreement. Where Data Processor believes that an instruction would be in breach of applicable law, Data Processor shall notify Data Controller of such belief without undue delay.

2.4. CATEGORIES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS. Data Controller may submit Personal Data to the Subscription Service as Customer Data, the extent of which is determined and controlled by Data Controller in its sole discretion and is further described in Appendix 1.

3. DATA CONTROLLER

3.1. COMPLIANCE WITH DATA PROTECTION LAWS. Data Controller shall comply with all of its obligations under Data Protection Laws when Processing Personal Data.

3.2. SECURITY RISK ASSESSMENT. Data Controller agrees that in accordance with Data Protection Laws and before submitting any Personal Data to the Subscription Service, Data Controller will perform an appropriate risk assessment to determine whether the security measures within the Subscription Service provide an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Data Controller is solely responsible for determining the adequacy of the security measures within the Subscription Service in relation to the Personal Data Processed. As further described in Section 7.1 (Product Capabilities) of the Data Security Guide, the Subscription Service includes, without limitation, column level encryption functionality and role-based access control, which Data Controller may use in its sole discretion to ensure a level of security appropriate to the risk of the Personal Data. For clarity, Data Controller may influence the scope and the manner of Processing of its Personal Data by its own implementation, configuration and use of the Subscription Service, including any other products or services offered by Brightfin and ServiceNow third-party integrations.

3.3. CUSTOMER’S AFFILIATES. The obligations of Data Processor set forth herein will extend to Customer’s Data Controller Affiliates to which Customer provides access to the Subscription Service or whose Personal Data is Processed within the Subscription Service, subject to the following conditions:

3.3.1. **Compliance**. Customer shall at all times be liable for its Affiliates’ compliance with this DPA and all acts and omissions by a Data Controller Affiliate are considered acts and omissions of Customer; and

3.3.2. **Claims**. Customer’s Data Controller Affiliates will not bring a claim directly against Data Processor. In the event a Data Controller Affiliate wishes to assert a valid legal action, suit, claim or proceeding against Data Processor (a “**Data Controller Affiliate Claim**”): (i) Customer must bring such Data Controller Affiliate Claim directly against Data Processor on behalf of such Data Controller Affiliate, unless Data Protection Laws require that Data Controller

Affiliate be party to such Data Controller Affiliate Claim; and (ii) all Data Controller Affiliate Claims will be considered claims made by Customer and are at all times subject to any aggregate limitation of liability set forth in the Agreement.

3.4. **COMMUNICATION.** Unless otherwise provided in this DPA, all requests, notices, cooperation and communication, including Instructions issued or required under this DPA (collectively, "**Communication**"), must be in writing and between Customer and Brightfin only and Customer shall inform the applicable Data Controller Affiliate of any Communication from Brightfin pursuant to this DPA. Customer shall be solely responsible for ensuring that any Communications (including Instructions) it provides to Brightfin relating to Personal Data for which a Customer Affiliate is Data Controller reflect the relevant Customer Affiliate's intentions.

3.4.1. **Notice.** All notices, requests, demands and determinations under this DPA (other than routine operational communications), will be in writing and will be deemed duly given (a) when delivered by hand, (b) one (1) day after being given to an express courier with a reliable system for tracking delivery, (c) when sent by confirmed facsimile or electronic mail with a copy sent by another means specified in this Section 3.4.1, or (d) six (6) days after the day of mailing, when mailed by United States mail, registered or certified mail, return receipt requested, postage prepaid, and addressed as follows:

To Brightfin: Brightfin
10731 E. Easter Ave, Suite #105
Centennial, CO 80112
ATTN: Legal
legal@brightfin.com

To Customer: [REDACTED]

4. DATA PROCESSOR

4.1. **DATA CONTROLLER'S INSTRUCTIONS.** Data Processor will have no liability for any harm or damages resulting from Data Processor's compliance with Instructions received from Data Controller. Where Data Processor believes that compliance with Data Controller's Instructions could result in a violation of Data Protection Laws or is not in the ordinary course of Data Processor's obligations in operating the Subscription Service, Data Processor shall promptly notify Data Controller thereof. Data Controller acknowledges that Data Processor is reliant on Data Controller's representations regarding the extent to which Data Controller is entitled to Process Personal Data.

4.2. **DATA PROCESSOR PERSONNEL.** Use of Customer's Personal Data by Data Processor will be limited to personnel who require such use to perform Data Processor's obligations under the Agreement and who are bound by obligations to maintain the confidentiality of such Personal Data.

4.3. **DATA SECURITY MEASURES.** Without prejudice to Data Controller's security risk assessment obligations under Section 3.2 (Security Risk Assessment) above, and 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, Data Processor shall maintain appropriate technical and organizational safeguards to protect the security, confidentiality and integrity of Customer Data, including any Personal Data contained therein, as described in Section 2 (Physical, Technical

and Administrative Security Measures) of the Data Security Guide. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction, and include:

4.3.1. **Service Access Control.** The Subscription Service provides user and role based access controls. Data Controller is responsible for configuring such access controls within its instance.

4.3.2. **Logging and Monitoring.** The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

4.3.3. **Testing.** Data Processor regularly tests, assess and evaluates the effectiveness of its information security program and may periodically review and update the such program to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

4.4. **DELETION OF PERSONAL DATA.** Upon termination or expiration of the Agreement, Data Processor shall return or - upon Data Controller's instruction - delete Customer Data, carrier media and other materials including Personal Data contained therein, as described in the Agreement.

4.5. **OBLIGATIONS** Data Processor shall support Data Controller in fulfilling data subjects' requests and claims, as detailed in Chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 32 to 36 GDPR. This includes inter alia:

4.5.1. using commercially reasonable efforts to ensure an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights through vulnerabilities, and enable the prompt detection of relevant injury events;

4.5.2. the obligation to report violations of Personal Data to the client without undue delay;

4.5.3. the obligation to assist the contracting entity in providing information to the person concerned, and to provide him with all relevant information without delay in that connection;

4.5.4. the support of the client for its data protection impact assessment; and

4.5.5. the assistance of the contracting authority in the context of prior consultations with the supervisory authority.

5. REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES

5.1. **REQUESTS FROM DATA SUBJECTS.** During the Subscription Term, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase or block Personal Data, or to transfer or port such Personal Data, within the Subscription Service, as may be required under Data Protection Laws (collectively, "**Data Subject Requests**").

5.2. RESPONSES. Data Controller will be solely responsible for responding to any Data Subject Requests, provided that Data Processor shall reasonably cooperate with the Data Controller to respond to Data Subject Requests to the extent Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Subscription Service. Data Processor will instruct the Data Subject to contact the Customer in the event Data Processor receives a Data Subject Request directly.

5.3. REQUESTS FROM AUTHORITIES. In the case of a notice, audit, inquiry or investigation by a government body, data protection authority or law enforcement agency regarding the Processing of Personal Data, Data Processor shall promptly notify Data Controller unless prohibited by applicable law. Data Controller shall keep records of the Personal Data Processed by Data Processor, and shall cooperate and provide all necessary information to Data Processor in the event Data Processor is required to produce such information to a data protection authority.

5.4. COSTS. Customer shall reimburse Brightfin for any reasonable additional costs incurred in connection with the fulfilment of Brightfin's obligations under Sections 5.2 and 5.3 above.

6. BREACH NOTIFICATION

Data Processor shall report to Data Controller any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data that it becomes aware of without undue delay.

7. MONITORING RIGHTS

No more than once annually, Data Controller may audit Data Processor's Processing of Personal Data under this DPA by exercising its audit rights set forth in Section 4.2 (Audits) and Section 4.4 (Corrective Actions) of the Data Security Guide.

8. SUB-PROCESSORS

8.1. USE OF SUB-PROCESSORS. Data Controller authorizes Data Processor to engage Sub-Processors appointed in accordance with this Section 8 to support the provision of the Subscription Service and to deliver Services as described in the Agreement.

8.2. LIABILITY. Use of a Sub-Processor will not relieve, waive or diminish any obligation Data Processor has under the Agreement, and Data Processor is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Data Processor.

9. INTERNATIONAL DATA TRANSFERS

9.1. STANDARD CONTRACTUAL CLAUSES AND ADEQUACY. Where required under Data Protection Laws, Data Processor or Data Processor's Affiliates shall require Sub-Processors to abide by (i) the Standard Contractual Clauses for Data Processors established in third countries; or (ii) another lawful mechanism for the transfer of Personal Data as approved by the European Commission.

9.2. PRIVACY SHIELD. Brightfin's Affiliate MobiChord, Inc. is a signatory to the EU-U.S. and Swiss-U.S. Privacy Shield Framework (the "**Framework**") set forth by the United States Department of Commerce with respect to the Processing of Personal Data transferred from the European Economic Area and Switzerland (the "**EEA**") to the United States. Notwithstanding the validity of the Framework within the EEA, Brightfin shall cause MobiChord, Inc. to continue to comply with its obligations under the Framework for so long as the Framework is maintained by the United States Department of Commerce (or for so long as MobiChord, Inc. remains a signatory, whichever is earlier). For purposes of cross-border data transfers, Brightfin shall utilize, where applicable, the Standard Contractual Clauses for Data Processes described in Section 9.1 above.

9.3. Changes to Privacy Law. In the event changes in applicable Privacy Laws require measures in addition to those set forth in this Section 9, the Parties will work in good faith to adopt or amend updated practices and contractual provisions to comply with such changes.

10. DATA PROTECTION IMPACT ASSESSMENTS

Data Processor will, on request, provide Data Controller with reasonable information required to fulfill Data Controller's obligations under the General Data Protection Regulation (2016/679) ("**GDPR**") to carry out data protection impact assessments, if any, for Processing of Personal Data within the Subscription Service. Data Controller is solely responsible for any prior consultation with a supervisory authority required for Processing of Personal Data under GDPR.

11. GENERAL PROVISIONS

11.1. CONFIDENTIALITY. Data Controller may only disclose the terms of this DPA to a data protection or regulatory authority to the extent required by law or regulatory authority, provided however, that any such disclosure shall be limited to the minimum information necessary to satisfy such disclosure requirement. Data Controller shall use commercially reasonable efforts to ensure that data protection or regulatory authorities do not make this DPA public.

11.2. LIMITATION OF LIABILITY. Customer's remedies with respect to any breach by Brightfin of the terms of this DPA will be subject to any aggregate limitation of liability under the Agreement. The section of the Agreement titled "Limitations of Liability" (or equivalent) shall apply to all Affiliates in the Brightfin family of companies.

11.3. TERMINATION. This DPA shall terminate simultaneously and automatically with the termination of the Agreement or expiration of the Subscription Term where Customer does not renew. Notwithstanding the foregoing, Brightfin shall continue to secure Personal Data in accordance with the terms herein for so long as Brightfin has access to such Personal Data. Documentations serving as proof of proper data processing must be kept by Brightfin according to the respective retention periods beyond the end of the contract.

11.4. WAIVER AND MODIFICATIONS. A waiver of any right is only effective if it is in writing and only against the party who signed such writing and for the circumstances given. Any modification of this DPA must be in writing and signed by authorized representatives of both parties.

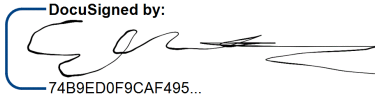
11.5. LEGAL EFFECT. This DPA shall only become legally binding between Customer and Brightfin upon Customer fully completing the steps set forth in “INSTRUCTIONS FOR EXECUTING THIS DPA.” The Section “Application of this DPA” specifies which Brightfin entity is party to this DPA. Notwithstanding the signatures below of any other Brightfin entity, such other Brightfin entities are not a party to this DPA. Customer shall at all times be responsible for its Affiliates’ compliance with this DPA.

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

Brightfin DPA 3.22.21

DATA PROCESSING AGREEMENT

The parties, each acting under due and proper authority, hereby execute this Data Processing Agreement as of the late date indicated below.

Customer:	Mobile Solutions Services, Holdings, LLC Inc., d/b/a Brightfin
Individual signing: (print name)	Individual signing: (print name) Ed Roshitsh
Signature:	Signature: 
Title:	Title: CEO
Signing Date:	Signing Date: 4/28/2021

Brightfin DPA 3.22.21

APPENDIX 1

DETAILS OF PROCESSING

Nature and Purpose of Processing

Data Processor will Process Personal Data as required to provide the Subscription Service and in accordance with the Agreement.

Duration of Processing

Data Processor will Process Personal Data for the duration of the Agreement and in accordance with Section 4 (Data Processor) of the DPA.

Data Subjects

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include Personal Data relating to the following categories of Data Subjects:

- Clients and other business contacts;
- Employees and contractors;
- Subcontractors and agents; and
- Consultants and partners.

Categories of Personal Data

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include the following categories:

- communication data (e.g. telephone number, mobile phone number, call detail records, email);
- business and personal contact details; (e.g. name, postal address)
- and other Personal Data submitted to the Subscription Service.

Special Categories of Personal Data

NOT APPLICABLE

Processing Operations

The Personal Data transferred will be subject to the following basic processing activities: all activities necessary for the performance of the Agreement.

DATA SECURITY GUIDE

1. SECURITY PROGRAM

While providing the Subscription Service, Brightfin will maintain a written information security program of policies and procedures governing the processing, storage, transmission and security of Customer Data (the “**Security Program**”). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Brightfin regularly tests, assesses and evaluates the effectiveness of the Security Program and may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

2. PHYSICAL, TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

2.1. PHYSICAL SECURITY MEASURES.

2.1.1. **Data Center Facilities.** Brightfin shall ensure that data centers used in the course of providing the Subscription Services have: (i) physical access restrictions and monitoring that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (ii) fire detection and fire suppression systems.

2.1.2. **Systems, Machines and Devices.** (i) Physical protection mechanisms; and (ii) entry controls to limit physical access.

2.1.3. **Media.** (i) Industry standard destruction of sensitive materials before disposition of media; (ii) secure safe for storing damaged hard disks prior to physical destruction; and (iii) physical destruction of all decommissioned hard disks storing Customer Data.

2.2. TECHNICAL SECURITY MEASURES.

2.2.1. **Access Administration.** Access to the Subscription Service by Brightfin employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g., the required use of complex passwords, and a two-factored authenticated connection) and is accessible for administration.

2.2.2. **Service Access Control.** The Subscription Service provides user and role based access controls. Customer is responsible for configuring such access controls within its instance.

2.2.3. **Logging and Monitoring.** The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

2.2.4. **Firewall System.** An industry-standard firewall is installed and managed to protect Brightfin systems by residing on the network to inspect all ingress connections routed to the Brightfin environment.

2.2.5. **Vulnerability Management.** Brightfin conducts periodic security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, Brightfin will obtain the patch from the applicable vendor and apply it within an appropriate timeframe.

2.2.6. **Antivirus.** Brightfin updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

2.2.7. **Change Control.** Brightfin ensures that changes to applications and production infrastructure are evaluated to minimize risk and are implemented following ServiceNow's standard operating procedure.

2.3. ADMINISTRATIVE SECURITY MEASURES.

2.3.1. **Personnel Security.** Brightfin performs background screening on employees and contractors who have access to Customer Data in accordance with Brightfin's then current applicable standard operating procedure and subject to applicable law.

2.3.2. **Security Awareness and Training.** Brightfin shall maintain a security awareness program that includes appropriate training of personnel on the Security Program. Training is conducted during onboarding and periodically throughout employment at Brightfin.

2.3.3. **Vendor Risk Management.** Brightfin shall maintain a vendor risk management program that assesses all vendors that access, store, process or transmit Customer Data for appropriate security controls and business disciplines.

3. **SERVICE CONTINUITY**

3.1. DATA CENTERS; DATA BACKUP. As of the Effective Date, all Customer Data is stored in ServiceNow Data Centers, backed up in accordance with ServiceNow's then-current information security protocols.

3.2. DISASTER RECOVERY. Brightfin shall ensure that any infrastructure or hosting provider used to provide the Subscription Service including, but not limited to Amazon Web Services, maintains industry standard disaster recovery and business continuity practices, policies and procedures.

3.3. PERSONNEL. In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to a Brightfin support representative, geographically distributed to ensure business continuity for support operations.

4. CERTIFICATIONS AND AUDITS

4.1. CERTIFICATIONS AND ATTESTATIONS. Brightfin shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001:2013 (or equivalent standards) (collectively, the “**Standards**”) for the information security management system supporting the Subscription Service. At least once per calendar year, Brightfin shall obtain an assessment against such Standards by an independent third-party auditor.

4.2. AUDITS. Upon Customer’s reasonable request, and no more than once annually, Brightfin shall grant Customer access to documentation evidencing the Security Program (“**Audit**”). Such Audit will include a copy of Brightfin’s certification or audit reports performed by an independent third-party of Brightfin’s information security management system supporting the Subscription Service against the Standards.

4.3. INSPECTIONS. No more than once annually, Customer has the right to: (i) carry out inspections in consultation with Brightfin or to have them carried out by examiners to be named on a case-by-case basis; (ii) verify Brightfin’s compliance with its obligations according to Art. 28 GDPR by way of random examinations; and (iii) provide the Customer with the required information and to provide information necessary to prove compliance with the obligations under Art. 28 GDPR, in particular the implementation of the technical and organizational measures.

4.4. CORRECTIVE ACTIONS. Brightfin and Customer may schedule a mutually convenient time to discuss the Audit. If a material deficiency is discovered between Brightfin’s commitments in this Data Security Guide and the information gathered during an Audit, then Brightfin shall take, at its own cost, the necessary corrective actions. This sets forth Customer’s exclusive rights and remedies (and Brightfin’s sole liability) with respect to any material deficiencies noted during an Audit. The Audit and the results derived therefrom are Confidential Information of Brightfin.

5. MONITORING AND INCIDENT MANAGEMENT

5.1. INCIDENT MONITORING AND MANAGEMENT. Brightfin will monitor, analyze and respond to security incidents in a timely manner in accordance with Brightfin’s standard operating procedure. Brightfin’s security group will escalate and engage response teams as may be necessary to address an incident.

5.2. BREACH NOTIFICATION. Unless notification is delayed by the actions or demands of a law enforcement agency, Brightfin will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a “**Breach**”) without undue delay following determination by Brightfin that a Breach has occurred.

5.3. REPORT. The initial report will be made to Customer security or privacy contact(s) (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available to Brightfin, and unless prohibited by applicable law, Brightfin shall provide without undue delay any further relevant information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Brightfin contact from whom additional information may

be obtained. Brightfin shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

5.4. CUSTOMER OBLIGATIONS. Customer will cooperate with Brightfin in maintaining accurate contact information and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s) and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

6. PENETRATION TESTS

Brightfin shall perform or contract with a third-party vendor to perform a penetration test on the application on a regular basis (at least annually) to identify risks and remediation that help increase security.

7. SHARING THE SECURITY RESPONSIBILITY

7.1. PRODUCT CAPABILITIES. The Subscription Service has the capabilities to: (i) authenticate users before access; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service. Customer shall be responsible for implementing encryption and access control functionalities available within the Subscription Service for protecting all Customer Data containing sensitive data and any Personal Data deemed sensitive or "special categories of personal data" under Data Protection Laws. Customer is solely responsible for its decision not to encrypt such data in ServiceNow and Brightfin will have no liability to the extent that damages would have been mitigated by Customer's use of such encryption measures. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Subscription Service.

7.2. CUSTOMER COOPERATION. Customer shall promptly apply any application upgrade that Brightfin and/or ServiceNow, as applicable, determines is necessary to maintain the security, performance or availability of the Subscription Service. For the avoidance of doubt, where upgrades are determined to be necessary by both Brightfin and ServiceNow, failure to apply both upgrades may result in the Subscription Services not functioning as intended.

7.3. LIMITATIONS. Notwithstanding anything to the contrary in this Data Security Guide or other parts of the Agreement, Brightfin's obligations extend only to those systems, networks, network devices, facilities and components over which Brightfin exercises control. This Data Security Guide does not apply to: (i) information shared with Brightfin that is not data stored in its systems using the Subscription Service; (ii) data in Customer's VPN or a third-party network; (iii) any data processed by Customer or its users in violation of the Agreement or this Data Security Guide; or (iv) Integrated Products. For the purposes of this Data Security Guide, "**Integrated Products**" shall mean ServiceNow-provided integrations to third-party products or any other third-party products that are used by Customer in connection with the Subscription Service. Customer agrees that its use of such Integrated Products will be: (a) in compliance with all applicable laws, including but not limited to, Data Protection Laws; and (b) in accordance with its contractual agreement with the provider of such Integrated Products. Any Personal Data populated from the Integrated Products to the Subscription Service must be collected, used,

disclosed and, if applicable, internationally transferred in accordance with Customer's privacy policy, which will adhere to Data Protection Laws. For clarity, as between Brightfin and Customer, Customer assumes all liability for any breaches of confidentiality that occur outside of the Subscription Service.