dun & bradstreet

SERVICE PROVIDER PRIVACY REQUIREMENT

Service Provider shall be required to secure the Personal Data that Service Provider Processes in accordance with the privacy requirements described below (referred as "Requirement" below).

Last update: June 30, 2022

1. Compliance with Applicable Privacy Laws

1.1 Service Provider shall not sell, for monetary or other valuable consideration, Personal Data provided by D&B without D&B's explicit, written consent.

1.2 Service Provider shall Process, retain, use, disseminate, disclose, make available, Transfer, or otherwise communicate orally, in writing, or by electronic or other means D&B Personal Data only on behalf of D&B and only as necessary to fulfill the business purpose as described in the Agreement and/or SOW.

1.3 Service Provider warrants that: (i) Provided Data collected in the United States or relating to residents or citizens of the United States was not collected for the purpose of, or used in any manner that would cause such Provided Data to be construed as, a "Consumer Report" as defined in 15 U.S.C. § 1681a; (ii) Provided Data was not collected, generated, compiled and/or obtained by illegal and/or abusive means, including but not limited to, web scraping, web mining, e-mail harvesting, "dictionary attacks" or e-mail modeling; (iii) Provided Data was collected in accordance with applicable Privacy Laws related to the collection and compilation of data and information; (iv) there are no material suits, claims, charges or proceedings currently pending or threatened against Service Provider relating to Provided Data; (v) there are no writs, injunctions, judgments, orders or decrees, nor any pending investigations of any governmental entity, against Service Provider relating to the Provided Data; and (vi) it is in compliance with all applicable Laws including, but not limited to, those relating to anti-corruption, fraud, bribery, export controls and trade sanctions.

1.4 Service Provider warrants that: (i) any and all Processing activities of Personal Data carried out by Service Provider for the purpose of gathering the Provided Data have been carried out in compliance in all material respects with applicable Privacy Law; (ii) any Personal Data Processed for the purposes under (i) above, have been obtained and collected (and will be obtained and collected from the relevant data subjects or from other authorized sources (including but not limited to Data User), in compliance in all material respects with applicable Privacy Law; (iii) Service Provider has provided to all data subjects (whose Personal Data is Processed as per (i) above) any applicable information, notices or documentation about the above Processing activities, and has obtained (or will obtain, as appropriate) any necessary consents, authorizations or approvals from such data subjects (or from any competent data protection authority) and has complied (or will comply, as appropriate) with any further requirements provided under applicable Privacy Law; and (iv) when Processing Provided Data, Service Provider has documented and effective procedures for addressing requests to access, delete and correct Personal Data in compliance with applicable Privacy Laws. Service Provider shall record and keep the notice provided to, and the written, electronic, or verbal consent obtained from each individual regarding the Processing of his/her Personal Data, any data subject requests received and/or fulfilled in relation to Provided Data, and the security measures implemented to store such Personal Data. Upon D&B's written request, Service Provider shall deliver all such records to D&B.

1.5 California Consumer Privacy Act (CCPA).Service Provider warrants that: (i) their privacy notice is up to date and accessible; (ii) it provides California consumers (as defined under the CCPA) with the option to "Opt Out" of the sale of their Personal Data under CCPA; and (iii) Service Provider will honor any CCPA deletion requests passed on by D&B. To receive or pass on CCPA requests, Service Provider will register at https://support.dnb.com/?prod=CCPARequests.

2. Requests for Access:

2.1 Notification: Service Provider must notify D&B in writing in the manner set forth in the Agreement, as soon as reasonably practicable and in any event within three (3) business days of any of the following occurrences:

(i) Service Provider receives a request for access from an individual to whom the D&B Personal Data or D&B Customer Data relates, or a legally authorized representative of that individual, to any Personal

Data Processed by Service Provider pursuant to the exercise of any legal right of access or where related to any complaint about the Processing of Personal Data by Service Provider;

(ii) Service Provider receives a request for access from any government official or judicial or administrative proceeding ("Government Requests") to any D&B Personal Data or D&B Customer Data Processed by Service Provider, where not legally prohibited from doing so; or

(iii) Service Provider receives any other request related to Personal Data from Third Parties.

2.2 Service Provider Responses to Requests:

(i) Service Provider shall have documented and effective procedures for addressing requests to access, delete and correct Personal Data in compliance with Privacy Laws. Service Provider shall honor such requests in compliance with Privacy Laws.

(ii) Except for Government Requests, Service Provider is not authorized to respond the request related to D&B Personal Data or D&B Customer Data unless explicitly authorized by D&B in writing or where obliged by applicable Privacy Laws, in which case Service Provider shall cooperate fully with D&B in preparing the response.

(iii) With respect to Government Requests, Service Provider shall cooperate fully with D&B in any effort led by D&B to intervene and quash or limit such requests or respond to a governmental authority relating to the D&B Personal Data or D&B Customer Data Processed by Service Provider under the Agreement. Should Service Provider be legally required to respond to a Government Request, Service Provider, after consultation with D&B, shall only disclose the minimum amount of Personal Data necessary to comply with Law or judicial process.

3. Service Provider Employees:

3.1 Background Checks: Where Permitted pursuant to applicable Privacy Laws, Service Provider will conduct and complete appropriate background and/or verification checks of its Employees that will be involved in the Processing of Personal Data pursuant to the Agreement. Service Provider shall ensure that no Employee shall Process Personal Data pursuant to the Agreement unless the results of such checks show no issues or any issues identified have been reviewed and deemed acceptable by Service Provider.

3.2 Training: Once a year and during Employee onboarding, Service Provider shall provide its Employees involved with Processing Personal Data in the performance of the Services under the Agreement with training on privacy, confidentiality and security appropriate to address Service Provider's obligations pursuant to the Agreement

3.3 Minimum Necessary: Service Provider shall make Personal Data provided by D&B available to Employees only to the extent and for the duration for which such availability or access is reasonably necessary to perform the Services under the Agreement.

4. Subcontractors and Other Third Parties:

4.1 Service Provider may not engage outside third parties or other non-Employees ("Subcontractors") to Process D&B Personal Data or D&B Customer Data in connection with the Services provided under the Agreement without the prior written approval of D&B.

4.2 Should Subcontractors be permitted to Process or Transfer Personal Data disclosed to Service Provider by or on behalf of D&B in connection with the Agreement, Service Provider shall (i) conduct a due diligence assessment of the privacy practices of the Subcontractor and (ii) execute a written agreement with each Subcontractor that includes provisions that require Subcontractor to adhere to the same or greater privacy, data security (including, without limitation, the background check requirements and the EU Data Model Clauses, as set forth at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010D0087, if these are deemed necessary and which makes D&B an intended beneficiary of that written agreement).

5. Return or Destruction of Personal Data: To the extent not otherwise prohibited by applicable Privacy Laws, at any time upon D&B's request, Service Provider shall immediately return to D&B and/or securely destroy all originals and copes of D&B Personal Data or D&B Customer Data in its possession, custody or control or the possession, custody or control of an Subcontractor return and/or destruction of Personal Data provide by D&B will be completed in accordance with Privacy Laws. For the avoidance of doubt,

Service Provider shall timely return, destroy or delete Personal Data when it is no longer necessary for the purpose to fulfill the service in the Agreement and/or SOW. Service Provider shall send D&B, within fifteen (15) days of D&B's request, a written certification signed by the Service Provider, acknowledging that all Personal Data Processed under the Agreement has been returned or securely destroyed consistent with the requirements of the Agreement and Privacy Laws. Personal Data will be retained for no longer than necessary to fulfill the Services provided under the Agreement.

6. Privacy and Security Audits:

6.1 Audit: In addition to the audit provisions in the Agreement, Service Provider shall provide D&B, D&B's authorized representatives, and/or applicable regulatory authorities having the right to carry out an audit of D&B, on reasonable notice, the right to audit Service Provider's business processes and practices involving the privacy, security and/or Processing of Personal Data in the performance of the Agreement, on at least an annual basis and following each occurrence of a Security Event.

6.2 Cost: D&B shall bear the full cost and expense of any such audit, unless such audit discloses any material weakness reasonably likely to give rise to a Security Event ("Security Issue"), in which case Service Provider shall bear the full cost and expense of such an audit.

6.3 Remediation: To the extent that a Security Issue is identified by an audit or otherwise discovered by or made known to Service Provider, Service Provider shall immediately notify D&B in writing and, within ten (10) business days thereafter, either remediate such Security Issue or provide D&B with a plan acceptable to D&B for Service Provider to remediate the Security Issue.

7. Privacy or Security Events:

7.1 Remediation:

(i) Service Provider shall take measures to protect Personal Data it processes under the Agreement or SOW. Within 24 hours of becoming aware of a Security Event, Service Provider shall inform D&B at security@dnb.com and PrivacyOfficerCH@dnb.com providing D&B with sufficient information to meet any obligations to report or inform data subjects of the Security Event under Applicable Laws. Such notification shall as a minimum:

(a) describe the nature of the Security Event, the categories and numbers of data subjects concerned, and the categories and numbers of Personal Data records concerned;

(b) communicate the name and contact details of Service Provider's data protection officer or other relevant contact from whom more information may be obtained;

(c) describe the likely consequences of the Security Event;

(d) describe the measures taken or proposed to be taken to address the Security Event; and

(e) the corrective action taken or proposed to be taken by Service Provider

(ii) Service Provider shall cooperate in good faith regarding actions that need to be taken to remediate, which may be required by Privacy Laws or which may otherwise be necessary, reasonable or appropriate under the circumstances, commensurate with the nature of the Security Event ("Remediation Efforts"). Service Provider shall share all pertinent information with D&B. If D&B has additional questions around the Security Event, Service Provider will attempt in good faith to answer any such questions. Remediation Efforts required by applicable Privacy Laws must be carried out and are not dependent upon the completion of the consultation process, although the Parties shall use good faith efforts to discuss Remediation Efforts required by applicable Privacy Laws during the consultation process.

(iii) Failure by Service Provider to take Remediation Efforts shall be deemed a material breach of the Agreement.

(iv) Pursuant to the consultation process, Service Provider shall undertake Remediation Efforts at its sole expense.

7.2 Cooperation: Service Provider shall keep D&B apprised of and cooperate reasonably with D&B in connection with D&B's investigation or any investigation by any regulatory or government authority of

any Security Event. Service Provider shall not make any public announcements or notify affected individuals regarding such Security Event without D&B's prior written approval unless it is required to do so pursuant to Privacy Laws, in which case it shall provide D&B reasonable prior notice where not prohibited by applicable Privacy Laws from doing so.

7.3 Indemnification: In addition to any other Indemnification provisions in the Agreement, Service Provider shall indemnify, defend and hold harmless D&B from and against any and all liability, loss, claim, injury, damage, penalty, fine, settlement or expense (including, without limitation, costs of Remediation Efforts and reasonable attorneys' fees and costs arising from, or relating to, any action, claim or allegation of a third party including, without limitation, any regulatory or government authority) of or with respect to any Security Event involving Personal Data.

8. Restricted Transfer

8.1 To the extent that the processing of Personal Data involves a Restricted Transfer, the parties undertake to provide the additional legal protections to the extent required by Privacy Law.

8.2 General Data Protection Regulations (GDPR).

(i) Controller to Processor. Service Provider warrants that to the extent D&B Personal Data subject to European Privacy Legislation is transferred to Service Provider under the Agreement, such Personal Data will be used and Processed in accordance with the EU Data Standard Contractual Clauses, as set forth at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en, or any future version of the EU Data Standard Contractual Clauses as required based on the nature of the Agreement under applicable law, which are incorporated herein by reference ("Data Transfer Agreement"). D&B shall be the Controller and the data exporter, and Service Provider shall be the Processor and data importer. The Data Transfer Agreement is governed by the laws of the Republic of Ireland. The Supervisory Authority shall be the Irish Data Protection Commission. For the purpose of Appendix 1 to the Data Transfer Agreement: (1) the use of sub-processors shall be in accordance with specific prior authorization. (2) the data subjects are those individuals whose Personal Data is provided to Service Provider in accordance with the Agreement and/or SOW between the Parties; (3) the categories of data are the categories of Personal Data provided to Service Provider in accordance with the Agreement and/or SOW between the Parties; (4) the special or sensitive categories of data (if any) to be Processed as defined by European Privacy Legislation are set forth in the Agreement and/or SOW between the Parties; (5) the frequency of the transfer shall be continuous or as set forth in the SOW; (6) the Processing operations to be performed are as specified in the Agreement and/or SOW between the Parties (7) the purpose of the transfer shall be for D&B to obtain the benefit of the Services under the Agreement (8) the transfer of Personal Data to sub-processors, if any, shall be for the purpose of providing the Services to D&B under the Agreement. For the purpose of Appendix 2 to the Data Transfer Agreement, the description of the technical and organizational security measures implemented by the data importer in accordance with EU Data Standard Contractual Clauses 4(d) and 5(c) are set forth at https://www.dnb.com.hk/Vendor-Data-Security-Requirement/page.htm. The contact points for data protection queries are the parties' contacts for matters under this the applicable agreement between the Parties. To the extent the terms of the Data Transfer Agreement conflict with other terms of the applicable agreement between the parties, the terms of the Data Transfer Agreement will control.

(ii) Controller to Controller. D&B warrants that to the extent Service Provider Personal Data subject to European Privacy Legislation is transferred to D&B under the Agreement, such Personal Data will be used and Processed in accordance with the EU Data Standard Contractual Clauses, as set forth at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en, or any future version of the EU Data Standard Contractual Clauses as required based on the nature of the Agreement under applicable law, which are incorporated herein by reference ("Data Transfer Agreement"). Service Provider shall be the Controller and the data exporter, and D&B shall be the Controller and data importer. The Data Transfer Agreement is governed by the laws of the Republic of Ireland. The Supervisory Authority shall be the Irish Data Protection Commission. For the purpose of Appendix 1 to the Data Transfer Agreement: (1) the data subjects are those individuals whose Personal Data is provided to D&B in accordance with the Agreement and/or SOW between the Parties; (2) the categories of data are the categories of Personal Data provided to D&B in accordance with the Agreement and/or SOW between the Parties; (3) the special or sensitive categories of data (if any) to be Processed as defined by European Privacy Legislation are set forth in the Agreement and/or SOW between the Parties; (5) the frequency of the transfer shall be continuous or as set forth in the SOW; (6) the Processing operations to be performed are as specified in the Agreement and/or SOW between the Parties (7) the purpose of the transfer shall be for D&B to obtain the benefit of the Services under the Agreement. For the purpose of Appendix 2 to the Data Transfer Agreement, the description of the technical and organizational security measures implemented by the data importer in accordance with EU Data Standard Contractual Clauses

4(d) and 5(c) are set forth at https://www.dnb.com.hk/Vendor-Data-Security-Requirement/page.htm. The contact points for data protection queries are the parties' contacts for matters under the Agreement. To the extent the terms of the Data Transfer Agreement conflict with other terms of the applicable agreement between the Parties, the terms of the Data Transfer Agreement will control.

(iii) Processor to Processor. Service Provider warrants that to the extent D&B Customer Personal Data subject to European Privacy Legislation is transferred to Service Provider under the Agreement, such Personal Data will be used and Processed in accordance with the EU Data Standard Contractual Clauses, as set forth at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en, or any future version of the EU Data Standard Contractual Clauses as required based on the nature of the Agreement under applicable law, which are incorporated herein by reference ("Data Transfer Agreement"). D&B shall be the Processor and the data exporter, and Service Provider shall be the Processor and data importer. The Data Transfer Agreement is governed by the laws of the Republic of Ireland. The Supervisory Authority shall be the Irish Data Protection Commission. For the purpose of Appendix 1 to the Data Transfer Agreement: (1) the use of sub-processors shall be in accordance with specific prior authorization; (2) the data subjects are those individuals whose Personal Data is provided to Service Provider in accordance with the Agreement and/or SOW between the Parties; (3) the categories of data are the categories of Personal Data provided to Service Provider in accordance with the Agreement and/or SOW between the Parties; (4) the special or sensitive categories of data (if any) to be Processed as defined by European Privacy Legislation are set forth in the Agreement and/or SOW between the Parties; (5) the frequency of the transfer shall be continuous or as set forth in the SOW; (6) the Processing operations to be performed are as specified in the Agreement and/or SOW between the Parties (7) importer may process exporter's personal data as a Processor to support the exporter in the context of providing and/or supporting internal business operations, business decisioning data, analytics, and services to its Customers, in the areas of third party risk management and compliance, supplier management, commercial credit, and sales and marketing activities (8) the transfer of Personal Data to sub-processors, if any, shall be to support the exporter in the context of providing and/or supporting internal business operations, business decisioning data, analytics, and services to its Customers, in the areas of third party risk management and compliance, supplier management, commercial credit, and sales and marketing activities. For the purpose of Appendix 2 to the Data Transfer Agreement, the description of the technical and organizational security measures implemented by the data importer in accordance with EU Data Standard Contractual Clauses 4(d) and 5(c) are set forth at https://www.dnb.com.hk/Vendor-Data-Security-Requirement/page.htm. The contact points for data protection queries are the parties' contacts for matters under this the applicable agreement between the Parties. To the extent the terms of the Data Transfer Agreement conflict with other terms of the applicable agreement between the Parties, the terms of the Data Transfer Agreement will control.

8.3 Recommended Model Contractual Clauses (Hong Kong):

(i) Data User to Processor. Service Provider warrants that to the extent D&B Personal Data subject to PDPO is transferred to Service Provider under the Agreement, such Personal Data will be used and Processed in accordance with Recommended Model Contractual Clauses, as set forth at https://www.pcpd.org.hk//english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf, or any future version of the as required based on the nature of the Agreement under applicable law, which are incorporated herein by reference ("RMCC"). D&B shall be the Data User and the data transferor, and Service Provider shall be the Processor and data transferee.

(ii) Data User to Data User. Service Provider warrants that to the extent Service Provider Personal Data subject to PDPO is transferred to Service Provider under the Agreement, such Personal Data will be used and Processed in accordance with Recommended Model Contractual Clauses, as set forth at https://www.pcpd.org.hk//english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf , or any future version of the as required based on the nature of the Agreement under applicable law, which are incorporated herein by reference ("RMCC"). Service Provider shall be the Data User and the data transferor, and D&B shall be the Data User and data transferee.

9. Definition

9.1 "Agreement" means the agreement signed between D&B and Service Provider.

9.2 "Controller"/ "Data User" shall have the meaning afforded to it under Privacy Laws

9.3 "D&B Customer Data" shall solely apply to Personal Data provided by D&B's customer as the controller to D&B as the processor for the limited purpose of supporting the customer in the context of providing and/or supporting internal business operations, business decisioning data, analytics, and services

in the areas of third party risk management and compliance, supplier management, commercial credit, and sales and marketing activities.

9.4 "Employee" means the employees of Service Provider, sub-contractors of Service Provider and employees of sub-contractors.

9.5 "European Privacy Legislation" means European Union Regulation 2016/679 and any other applicable European data protection legislation including implementing legislation, guidelines and industry standards from time-to-time in force in a relevant jurisdiction, relating to the use and Processing of Personal Data in that jurisdiction.

9.6 "Law" means applicable national, international and local laws, statutes, rules, regulations and ordinances.

9.7 "Personal Data" shall have the meaning afforded to it under applicable Privacy Laws, including, but not limited to, Personal Data Privacy Ordinance (Cap 486.), European Privacy Legislation.

9.8 "PDPO" means Personal Data (Privacy) Ordinance (Cap. 486) in Hong Kong.

9.9 "Privacy Laws" means all Laws applicable to governing the privacy, security, confidentiality and protection of personally identifiable information including but not limited to Personal Data (Privacy) Ordinance (Cap. 486), European Privacy Legislation etc.

9.10 "Process", "Processed" or "Processing" means any operation, or set of operations, which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, use, disclosure by transmission, transmission or otherwise making available, alignment or combination, return or destruction.

9.11 "Processor" shall have the meaning afforded to it under Privacy Laws.

9.12 "Provided Data" means any data or information: (i) uploaded, submitted, posted, transmitted or otherwise provided or made available to D&B by Company; (ii) collected, downloaded or otherwise received by Company for or on behalf of D&B pursuant to the Agreement; or (iii) based on or derived from any of the foregoing in (i)-(ii), including any statistical or other analysis, as well as copies, improvements, modifications, adaptations, translations and other derivative works of, based on, derived from or otherwise incorporating any of the foregoing in (i)-(ii).

9.13 "D&B Customer Data" shall solely apply to Personal Data provided by D&B's customer as the controller to D&B as the processor for the limited purpose of supporting the customer in the context of providing and/or supporting internal business operations, business decisioning data, analytics, and services in the areas of third party risk management and compliance, supplier management, commercial credit, and sales and marketing activities.

9.14 "Security Event" means: (i) Confidential Information, or IT Assets have been or are likely to be accessed or used by any unauthorized Person including but not limited to incidents resulting from or arising out of internal use, Processing, or Transfer of Personal Data including by any Subcontractor; (ii) there has been or is likely to be any destruction, alteration or loss of information contained in or obtained from IT Assets, or (iii) any other incident as may be so defined by Privacy Laws.

9.15 "Services" means the services provided by Company, as set forth in a SOW, including any Deliverables.

9.16 "SOW" means the statement of work under the Agreement.

9.17 "Transfer" or "Transferred" means (a) the moving of Personal Data from one location or person to another, whether by physical or electronic means; and (b) granting of access to Personal Data by one location or person to another, by physical or electronic means.

9.18 "Restricted Transfer" shall mean a Transfer from one party to another party which would be prohibited by Privacy Law in the absence of additional legal protections as specified by Privacy Law.