dun & bradstreet

D&B Global Privacy Exhibit

Table of Contents

Global Privacy Exhibit

D&B and Customer (collectively the "Parties") have entered into a master agreement or an order referencing terms pertaining to the products included in such order (as applicable, the "Agreement") under which D&B may process Customer Personal Data and/or provide Customer with D&B Personal Data in connection with the provision of Services. This Global Privacy Exhibit, hereafter referred to as the "**GPE**", governs the processing, transfer and receipt of Personal Data under the Agreement. This GPE shall remain in effect at all times during the term of the Agreement, or after the term if either party retains access to the other party's Personal Data. This GPE shall form part of and be incorporated by reference into the Agreement. The Parties shall, and shall cause its Representatives to, comply with this GPE. In the event of a conflict between the GPE and the Agreement, this GPE shall prevail unless expressly preempted in the Agreement.

BACKGROUND

(A) Customer wishes to receive and D&B wishes to provide products or services under existing and/or future Agreement(s) between the parties (which includes contracts, order forms and statements of work);

(B) D&B may therefore:

i) Process (including transferring out of a jurisdiction) Customer Personal Data subject to Applicable Privacy Law on behalf of Customer as a consequence of the Agreement; and/or

ii) Transfer D&B Personal Data subject to Applicable Privacy Law to Customer for the Customer's use as set out in the Agreement;

(C) Certain Applicable Privacy Laws, including but not limited to the GDPR, provide for specific requirements around the Processing of such Personal Data;

(D) The Parties therefore, by executing the Agreement, enter into this GPE to satisfy such requirements;

(E) Applicable Privacy Law may require that such processing shall be governed by a written agreement;

(F) Any incorporation of the "Data Processing Agreement" by reference shall hereafter also incorporate this GPE.

(G) The parties therefore through completion of an Agreement enter into this GPE to satisfy such requirement;

(H) The parties may also require a lawful transfer mechanism to transfer (or fulfil onward obligations of a transfer) of Personal Data and where required have agreed to use the mechanism set out at Schedule 2 and/or Schedule 3.

(I) Schedules 1 and 2, are not applicable to Customer Personal Data processed by a D&B entity under the jurisdiction of European Union law or the laws of a jurisdiction deemed adequate by European Commission as set out at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en/.

(J) Schedules 1 and 3 are not applicable to D&B Personal Data processed by Customer under the jurisdiction of European Union law or the laws of a jurisdiction deemed adequate by European Commission as set out at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en/.

1. DEFINITIONS AND INTERPRETATION

The defined terms used in this GPE are found either in this clause 1 or elsewhere in the GPE or in the Agreement. For the purposes of this GPE, in the event of a conflict between a definition in the Agreement or the GPE, the GPE definition shall control.

"CCPA" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), and any related regulations or guidance provided by the California Attorney General.

"CCPA Requests" has the meaning set forth in the CCPA.

"Controller" shall have the meaning set forth under Applicable Privacy Law.

"Contact Information" means professional information D&B collects and compiles relating to a person in the context of business which may include but is not limited to names, titles, business phone, e-mail addresses and physical addresses.

"Customer Personal Data" shall mean Personal Data that is subject to Applicable Privacy Law and provided by or on behalf of Customer to D&B pursuant to the Agreement.

"D&B" shall mean the Dun & Bradstreet company named in the Customer's Agreement.

"D&B Personal Data" shall mean D&B owned or controlled Personal Data subject to Applicable Privacy Law which Customer licenses pursuant to the Agreement.

"Data Subject" shall have the meaning set forth under Applicable Privacy Law.

"GDPR"- Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data 2016/679

"Personal Data" shall have the meaning set forth under Applicable Privacy Law.

"Personal Data Breach" shall have the meaning set forth under Applicable Privacy Law.

"Applicable Privacy Law" shall mean any applicable data protection, data privacy and marketing legislation including implementing legislation, guidelines, and industry standards in force in a relevant jurisdiction. Relevant jurisdictions include but are not limited to the European Union, the European Economic Area including the United Kingdom (and Northern Ireland), Switzerland, Serbia, and Bosnia and Herzegovina. Applicable data protection and privacy legislation includes legislation relating to the use and processing of Personal Data including but not limited to the GDPR, the UK GDPR, the Switzerland Federal Act on Data Protection (FADP), the Singapore Personal Data Protection Act (PDPA), the China Personal Information Protection Law (PIPL), The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), The Virginia Consumer Data Protection Act (VCDPA) and other similar legislation, including any laws recognizing the protections set out under the Standard Contractual Clauses as a legally required and/or adequate data transfer mechanism. Applicable marketing legislation includes The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), the Telephone Consumer Protection Act of 1991 (TCPA), and other similar global legislation. Notwithstanding the foregoing, where a party is bound by sector specific privacy regulations, nothing in this GPE binds the other party to such regulations including but not limited to the Gramm-Leach-Bliley Act (GLBA) and NY DFS 23 NYCRR 500 "Cybersecurity Requirements for Financial Services Companies".

"Process" "Processing" and "Processed" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" shall have the meaning set forth under Applicable Privacy Law.

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

"Sensitive Personal Data" shall have the meaning specified under Applicable Privacy Law and may include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, a Social Security number, driver's license number, passport number or other government issued identification, account number, credit or debit card number, or personal identification number, login, or password that would permit access to the person's account or such other special categories defined as sensitive or subject to special protections under Applicable Privacy Law.

"Standard Contractual Clauses" shall mean the Annex to the Commission Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council or any subsequent version thereof.

"Standard Contractual Clauses Module I Controller to Controller" shall mean the Standard Contractual Clauses Module I set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en or any subsequent version thereof, incorporated in Schedule 3 hereto.

"Standard Contractual Clauses Module II Controller to Processor" shall mean the Standard Contractual Clauses Module II set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en or any subsequent version thereof, incorporated in Schedule 2 hereto.

"Sub-Processor" shall mean a third party contracted by D&B to process the Customer Personal Data on behalf of D&B for delivery of the Services to Customer.

"Services" means the data, software, and services identified in the Agreement between D&B and Customer.

"UK SCC Addendum" shall mean the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (vB1.0) issued by the UK Information Commissioner's Office or any subsequent version thereof.

2. SCOPE

2.1 This GPE applies to: 1) D&B Personal Data D&B provides to Customer; 2) Customer Personal Data which D&B Processes on behalf of Customer; 3) the transfer of Personal Data out of a jurisdiction; and 4) the receipt of Personal Data.

2.2 Details relating to the subject matter, duration, nature and purpose of Processing Personal Data under this GPE are as specified at Annex 1.B **Schedule 1** and the Agreement.

2.3 The Parties' transfer requirements for Restricted Transfers are set forth at **Schedule 2** and **Schedule 3.**

2.4 A list of D&B's sub-processors shall be as set out at **Schedule 4** and instructions for Customer registration for notifications and updates shall be as set out in clause 7.

2.5 D&B and Customer shall comply with any changes to this GPE that are necessary under Applicable Privacy Law.

3. COMPLIANCE

3.1 The Parties will comply with Applicable Privacy Law in their performance, receipt and use (as appropriate) of the Services.

3.2 The Controller is, in the capacity of the data controller, responsible for the personal data processed within the scope of the Agreement.

3.3 In its role as Processor of Customer Personal Data, D&B (i) will only act on documented instructions contained within the Agreement regarding the processing of Customer Personal Data, (ii) will not process Customer Personal Data for any purposes other than for the purpose(s) specified in the Agreement (iii) will not disclose Customer Personal Data to any third party unless permitted to do so under the Agreement and/or this GPE, is requested to do so by Customer in writing or is required by law. D&B shall notify Customer if it believes that the Customer's instructions infringe Applicable Privacy Law unless informing Customer is prohibited by law.

3.4 Where disclosure of Customer Personal Data is required by law, D&B will (to the extent permitted by law) inform Customer in advance of making the disclosure and will co-operate with Customer to limit the scope of the disclosure to what is strictly required by law.

3.5 Customer represents and warrants it is entitled under Applicable Privacy Law to provide Customer Personal Data to D&B to process as described herein.

3.6 Save where Customer's provision of such information forms an integral part of the relevant Services, Customer will not provide to D&B any Sensitive Personal Data

3.7 D&B certifies that D&B will comply with its obligations under the CCPA. D&B's privacy notice available at https://www.dnb.com/utility-pages/privacy-policy.html#title-fourteen may be used as documentation of D&B's compliance with CCPA notice obligations. D&B will honor any CCPA Requests passed on by Customer, where required to comply by the CCPA and CCPA regulations issued by the California Attorney General. To the extent that Customer provides to D&B Customer Personal Data subject to the CCPA, unless otherwise disclosed in writing and consented to by Customer, D&B will not sell such Customer Personal Data. D&B will process, retain, use, disseminate, disclose, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, such Customer Personal Data only on behalf of Customer and only as necessary to fulfill the business purpose under the Agreement. If applicable based on Customer's licensing of D&B Personal Data subject to the CCPA, Customer warrants that Customer will honor any CCPA Opt-out requests passed on by D&B. To receive or submit CCPA Requests, Customer will register at https://support.dnb.com/?prod=CCPARequests.

3.8 Each party will provide the other party with reasonable co-operation and assistance in relation to any complaint, request or other legal obligation under Applicable Privacy Law regarding the Services.

4. CONTACT INFORMATION

4.1 Contact Information may not have been obtained directly from Data Subjects and Data Subjects may not have opted in or otherwise expressly consented to receiving direct marketing, nor has D&B scrubbed Contact Information against wireless suppression lists, Do-Not-Call lists or other opt out lists (other than its own).

4.2 Prior to using Contact Information for direct marketing or any other permitted purposes, Customer should check all Applicable Privacy Law and shall be responsible for compliance with such Applicable Privacy Law in connection with Customer's use of the Contact Information. D&B may provide information regarding market-level compliance rules and restrictions (the "Compliance Insights") to help facilitate transparency and Customer compliance, however, D&B expressly disclaims any liability for use of, or reliance on, any such Compliance Insights. D&B shall not be liable for any damages, losses, costs, claims, or expenses arising from use thereof.

4.3 Contact Information may only be used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession. It is Customer's responsibility to observe any indicators D&B provides to Customer indicating the Data Subject has expressly objected to receiving direct marketing (as well as their own and any applicable opt out lists) prior to any direct marketing. Opt-out provisions and/or opt-out links in Customer's marketing and sales materials shall not pertain to opting out of D&B's marketing lists and/or databases. If Customer uses Contact Information in a manner that violates the foregoing requirements, D&B shall not be liable for any damages, losses, costs, claims or expenses arising therefrom.

5. CONFIDENTIALITY AND SECURITY

5.1 Having regard to the state of the art and cost of implementation, D&B will take appropriate technical measures (including the use of encryption) and organizational measures (including confidentiality obligations towards all staff working with Customer Personal Data) to avoid unauthorized or unlawful processing of Customer Personal Data and against accidental loss or destruction of or damage to Customer Personal Data taking into account the processing and the nature of the Customer Personal Data to be protected.

5.2 D&B will take reasonable steps in regard to the reliability of any of its employees who have access to the Customer Personal Data, including training all such employees in Applicable Privacy Law and requiring such employees to maintain confidentiality with respect to the Customer Personal Data. D&B will limit access to the Customer Personal Data (including when in a test environment) to those of its employees who have a business need for access.

5.3 If D&B becomes aware of a Personal Data Breach involving Customer Personal Data (the "Incident"), D&B will:

(i) promptly notify Customer of the details of the Incident to the email address registered by Customer at https://service.dnb.com (Select "My Dun & Bradstreet Subscription, "Manage My Product Notifications", "Create User" (or "Log In"), then go to the "Legal & Contractual" tab and select, ""Security Incident as per Contract");

(ii) promptly initiate an investigation into the circumstances surrounding the Incident and make a report of the investigation available to Customer; and

(iii) co-operate with Customer's investigation and at Customer's cost provide such reasonable assistance requested by Customer in order for Customer to comply with its obligations under Applicable Privacy Law including any notifications that Customer is required to make as a result of an Incident and

iv) not make a notification to a supervisory authority unless requested to do so in writing by Customer or otherwise required by Applicable Privacy Law.

6. COOPERATION

6.1 D&B will delete or return the Customer Personal Data if an account is terminated or not renewed unless Applicable Privacy Law requires storage of said Customer Personal Data.

6.2 Where required under Applicable Privacy Law, D&B shall make available to Customer information legally required to demonstrate compliance with this GPE.

6.3 D&B and Customer shall implement measures to assist each other in complying with the rights of the Data Subjects to the extent required under Applicable Privacy Law.

6.4 Where permitted by law, D&B will notify Customer promptly if D&B receives any enquiry or complaint from a supervisory authority or Data Subject about the processing of Customer Personal Data. D&B will co-operate with Customer to permit it to respond to such enquiry or complaint.

6.5 D&B shall also assist Customer in relation to (i) any data protection impact assessment or regulatory consultation that Customer is legally required to make in relation to Customer Personal Data; and (ii) the implementation of D&B's technical and organizational security measures as required under Applicable Privacy Law.

6.6 Where entitled under Applicable Privacy Law Customer may verify that Customer Personal Data processed by D&B under this GPE is processed in accordance with this GPE and the Agreement. D&B shall make available to Customer all information necessary to demonstrate such compliance. D&B shall also take measures for allowing, and contributing to audits, including inspections, conducted by Customer or a third party appointed by Customer. Such third party shall not be a direct competitor to D&B and shall have undertaken to comply with confidentiality obligations not less restrictive than those set out under the Agreement.

6.7 Customer shall no later than ten (10) business days prior to an intended inspection under clause 6.6 notify D&B thereof. Any such inspections shall be carried out during normal business hours. D&B shall be given at least fourteen (14) business days to respond to Customer's request for relevant information set out in clause 6.6 above.

6.8 Any other audits shall be managed as set out in the Agreement.

7. SUB-PROCESSORS OF CUSTOMER PERSONAL DATA

7.1 Customer acknowledges and agrees that D&B may use sub-processors to Process Customer Personal Data. D&B may continue to use such sub-processors already engaged by D&B as at the date of this GPE and listed at **Schedule 4** (subject to D&B in each case meeting the obligations set out in this GPE).

7.2 Customer will register and keep up to date in accordance with the relevant email address(es) of its personnel to receive written notice of new sub-processors (including full details of the processing to be undertaken). **To be notified of any change to our sub-processors, please register any applicable email addresses at support.dnb.com (select "My Dun & Bradstreet Subscription, "Manage My Product Notifications", "Create User" (or "Log In"), then go to the "Legal & Contractual" tab and select, "Change of Subcontractors").**

7.3 If on receipt of a notification received under clause 7.2 Customer notifies D&B in writing within five (5) working days of any objections (on reasonable grounds) to an appointment D&B shall halt the prospective Processing until reasonable steps have been taken to address the objections raised by Customer.

7.4 D&B shall enter into a written agreement or other binding legal act with each sub-processor which imposes materially the same obligations on that sub-processor as are imposed on D&B under this GPE and the Agreement.

7.5 D&B shall remain liable to Customer for any sub-processor's processing of the Customer Personal Data under this GPE and the Agreement to the extent such liability is required by Applicable Privacy Law.

8. RESTRICTED DATA TRANSFERS

8.1 To the extent that the processing of Customer Personal Data by D&B and/or any of its sub-processors involves a Restricted Transfer, the parties undertake to provide the additional legal protections to the extent required by Applicable Privacy Law. Such safeguards include (but are not limited to) the data transfer mechanisms set forth in **Schedule 2 and Schedule 3.** To the extent the terms of the Standard Contractual Clauses conflict with the Agreement or this GPE, the terms of the Standard Contractual Clauses will control.

9. GENERAL

9.1 This GPE shall be governed by and construed in accordance with the laws of the jurisdiction listed in the Agreement and those laws shall have exclusive jurisdiction to determine any disputes which may arise out of, under, or in connection with this GPE.

9.2 In the event that any one or more of the provisions of this GPE shall for any reason be held to be invalid, illegal or unenforceable, the remaining provisions of this GPE shall continue in full force and effect and the parties will negotiate in good faith to substitute a provision of like effect and intent to that deemed to be unenforceable.

Schedule 1: Annexes to the Standard Contractual Clauses

Annexes to the Controller to Processor Standard Contractual Clauses

Annex I.A LIST OF PARTIES

***Data exporter(s)*:**

Name: The Customer, as defined in the Agreement that incorporates these Standard Contractual Clauses by reference.

Address: As set forth in the Agreement that incorporates these Standard Contractual Clauses by reference.

Contact person's name, position and contact details: As set forth in the Agreement that incorporates these Standard Contractual Clauses by reference

Activities relevant to the data transferred under these Clauses: The Controller may provide personal data to the Processor to enable the Processor to cleanse, enrich, analyze, or expand upon such data for use by Controller in the areas of third party risk management and compliance, supplier management, commercial credit, and sales and marketing activities, as set forth in the Agreement that incorporates these Standard Contractual Clauses by reference.

Signature and date: These Standard Contractual Clauses have been incorporated into an Agreement between Controller and Processor, and are signed by virtue of the execution of the Agreement, and dated as of the effective date of the Agreement.

Role (controller/processor): Controller

***Data importer(s)*:**

Name: Dun & Bradstreet as defined in the Agreement.

Address: As set out in the Agreement

Contact person's name, position and contact details: Chief Privacy Officer at privacyofficer@dnb.com or EU Data Protection Officer at EUDPO@dnb.com

Activities relevant to the data transferred under these Clauses: Dun & Bradstreet may process Exporter's personal data in the context of providing business decisioning data, analytics, and services to Exporter, in the areas of third party risk management and compliance, supplier management, commercial credit, and sales and marketing activities.

Signature and date: These Standard Contractual Clauses have been incorporated into an Agreement between Controller and Processor, and are signed by virtue of the execution of the Agreement, and dated as of the effective date of the Agreement.

Role (controller/processor): Processor

Annex I.B DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Individuals associated or potentially associated with incorporated and unincorporated organisations

Categories of personal data transferred

Customer may provide the minimum required from the following list in order for D&B to provide the product or service requested: email addresses, names, contact details, job titles, residential or business address; photograph; employer; academic title and qualifications; career history; driving license; attendance records; job title; gender; date of birth; professional telephone number (including mobile telephone number) and fax number; personal email address; personal telephone number (including mobile telephone number); marital status; credit score or limit, risk, failure and delinquency score; payment information; D-U-N-S® Number; type of business; IP address; cookie data; login credentials (username and password); traffic data; images, sounds and other similar categories that are not Sensitive Personal Data.

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

Not applicable

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

Continuous

Nature of the processing

As outlined in the Agreement

Purpose(s) of the data transfer and further processing

Business information services

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

As set by Exporter

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

Storage and business processing

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

The technical and organizational measures including technical and organisational measures to ensure the security of the data, shall be as set out at https://www.dnb.com/about-us/company/our-security.html. The measures described therein may be updated but they shall not be made weaker than as set out on the date of signing of the Agreement.

Annex I.A LIST OF PARTIES

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

Name: Dun & Bradstreet as defined in the Agreement.

Address: As set out in the Agreement.

Contact person's name, position and contact details: Chief Privacy Officer, privacyofficer@dnb.com (EU Data Protection Officer EUDPO@dnb.com)

Activities relevant to the data transferred under these Clauses: Exporter is providing Personal Data in the context of providing business decisioning data, analytics, and services to Importer, in the areas of third party risk management and compliance, supplier management, commercial credit, and sales and marketing activities

Signature and date: These Standard Contractual Clauses have been incorporated into an Agreement between Importer and Exporter, and are signed by virtue of the execution of the Agreement, and dated as of the effective date of the Agreement.

Role (controller/processor): Controller

Data importer(s)*: [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: The Customer, as defined in the Agreement that incorporates these Standard Contractual Clauses by reference.

Address: As set forth in the Agreement that incorporates these Standard Contractual Clauses by reference.

Contact person's name, position and contact details: As set forth in the Agreement that incorporates these Standard Contractual Clauses by reference

Signature and date: These Standard Contractual Clauses have been incorporated into an Agreement between Importer and Exporter, and are signed by virtue of the execution of the Agreement, and dated as of the effective date of the Agreement.

Role (controller/processor): Controller

Annex I.B DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Individuals associated or potentially associated with incorporated and unincorporated organisations.

Categories of personal data transferred

email addresses, names, contact details, job titles, residential or business address; photograph; employer; academic title and qualifications; career history; driving license; attendance records; job title; gender; date of birth; professional telephone number (including mobile telephone number); personal telephone number (including mobile telephone number); marital status; credit score or limit, risk, failure and delinquency score; payment information; D-U-N-S® Number; type of business; IP address; cookie data; login credentials (username and password); traffic data; images, sounds and other similar categories that are not Sensitive Personal Data.

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

Not applicable

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

As outlined in the Agreement

Nature of the processing

As outlined in the Agreement

Purpose(s) of the data transfer and further processing

Performance of services pursuant to the Agreement.

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

As determined by Importer and for no longer than is necessary for the purposes for the purposes for which the personal data are processed

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

Annex I.C COMPETENT SUPERVISORY AUTHORITY

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

Data Protection Commission

21 Fitzwilliam Square

D02 RD28 Dublin 2

Tel. +353 76 110 4800

Email: info@dataprotection.ie

Website: http://www.dataprotection.ie/

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

Measures of encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

The technical and organizational measures of D&B shall be as set out at https://www.dnb.com/about-us/company/our-security.html

The technical and organizational measures of Customer shall be as set out in the Customer Data Privacy and Data Protection Safeguards Attestation as set out in Schedule 5.

The technical and organizational measures of the sub-processor shall be materially similar to those of the Controllers.

- ***Transfers (or onward transfers) of Personal Data from Customer Exporter to D&B as the Importer, where such Personal Data is subject to Applicable Privacy Law recognizing the protections set out under the Standard Contractual Clauses as a legally required and/or adequate data transfer mechanism, are subject to the Standard Contractual Clauses Module II Controller to Processor as set out in this Schedule 2.***
- ***Transfers (or onwards transfers) of UK Personal Data from Customer Exporter to D&B as the Importer are subject to the UK SCC Addendum, or any subsequent version thereof, which the Parties hereby incorporate by reference in unmodified form into this Schedule 2.***

STANDARD CONTRACTUAL CLAUSES - Module II Controller to Processor

The Standard Contractual Clauses Module II Controller to Processor shall be as set forth at Module II at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en, or any subsequent version thereof, which are incorporated herein by reference and as specified below.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 9

Use of Sub-Processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 10 working days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[1] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

[1] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A - LIST OF PARTIES

Data exporter(s)*:*

As set out in Schedule 1.

Data importer(s):

As set out in Schedule 1.

B - DESCRIPTION OF TRANSFER

As set out in Schedule 1.

C - COMPETENT SUPERVISORY AUTHORITY

To the extent Controller has a headquarters, regional headquarters, or affiliate in the EEA, the competent supervisory authority shall be the EU Member State in which such headquarters, regional headquarters, or affiliate (in that order of priority) is located.

To the extent Controller is not established in any EU Member State and has appointed a representative, the competent supervisory authority shall be the EU Member State in which such representative is located.

To the extent Controller is not established in any EU Member State and has not appointed a representative, the competent supervisory authority shall be the EU Member State of the applicable personal data subject.

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

The technical and organisational measures shall be as described in Schedule 1.

Schedule 3: Controller to Controller Standard Contractual Clauses

- **Transfers of Personal Data from D&B to Customer, where such Personal Data is subject to Applicable Privacy Law recognizing the protections set out under the Standard Contractual Clauses as a legally required and/or adequate data transfer mechanism, are subject to the Standard Contractual Clauses Module I Controller to Controller, as set out in this Schedule 3.**
- **Transfers of UK Personal Data from D&B to Customer are subject to the UK SCC Addendum, or any subsequent version thereof, which the Parties hereby incorporate by reference in unmodified form into this Schedule 3.**

STANDARD CONTRACTUAL CLAUSES - Module I Controller to Controller

The Standard Contractual Clauses Module I Controller to Controller shall be as set forth at Module I at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en, or any subsequent version thereof, which are incorporated herein by reference and as specified below.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A - LIST OF PARTIES

As set out at Schedule 1

B - DESCRIPTION OF TRANSFER

As set out at Schedule 1

C - COMPETENT SUPERVISORY AUTHORITY

As set out at Schedule 1

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

Measures of encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

The Technical and Organisational Measures for transfers to (sub-) processors shall be as set out at Schedule 1.

Schedule 4: Sub-Processors

D&B's current list of third party sub-processors is set forth at https://www.dnb.com/dnbsubprocessors. This list will be updated from time to time. You can register for notifications of sub-processor updates in accordance with the instructions in Section 7.2 of this Agreement.

Schedule 5: Customer Data Privacy and Data Protection Safeguards Attestation

Customer understands that Dun & Bradstreet is relying on its implementation of appropriate technical and organizational measures to protect Personal Data provided to Customer by Dun & Bradstreet. Customer has reviewed its obligations pursuant to its Agreement and this Schedule and attests that Customer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed and that Customer shall process the personal data only for the specific purpose(s) of the transfer as set out at Schedule 1.

Customer additionally attests that it has in place at least one of the following mechanisms to protect Personal Data:

- Binding Corporate Rules
- Privacy Shield Certification or the Trans-Atlantic Data Privacy Framework (as amended) upon coming into force
- APEC Cross-Border Privacy Rule Certification
- ISO 27001 Certification
- ISO 27701 Certification
- TRUSTe Privacy Certification
- VeraSafe Privacy Program Certification
- TÜV Data Protection Certification
- Bureau Veritas' Data Protection Certification
- GDPR Validation- EDAA Certification
- HITRUST CSF Certification
- JIPDEC PrivacyMark
- Other Privacy or Data Protection Certification or Trustmark
- SOC 2, Type II
- PCI DSS Attestation of Compliance
- EU Cloud Code of Conduct
- CSA CoC for GDPR Compliance
- CSA STAR
- ISO 27018 Certification
- ISO 27017 Certification
- APEC PRP Certification
- NIST Privacy Framework
- NIST Security Framework