dun & bradstreet

D&B Data Processing Agreement

BACKGROUND

(A) Customer processes personal data subject to Privacy Law in connection with their business activities;
(B) Customer wishes to receive and D&B wishes to provide goods and/or services under existing and/or future agreement(s) between the parties (the "**Master Agreement**" which includes order forms and statements of work and master terms governing those orders and statements of work);
(C) D&B may therefore process personal data subject to Privacy Law on behalf of Customer as a consequence of the Master Agreement;
(D) Customer may also receive from D&B personal data subject to Privacy Law compiled by D&B as part of the services provided by D&B under the Master Agreement;
(E) Privacy Law provides that such processing shall be governed by a written agreement;
(F) The parties therefore through completion of a Master Agreement enter into this Data Processing Agreement ("**DPA**") to satisfy such requirement;
(G) 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 3 and/or Schedule 5 and
(H) Customer will receive D&B's current DPA on each occasion it provides Personal Data to D&B.

1. DEFINITIONS AND INTERPRETATION

In this DPA, the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

Controller	as defined in Privacy Law
Cross-border Processing	as defined in Privacy Law
D&B	as defined in the Customer's Master Agreement
Data Subject Personal Data	as defined in Privacy Law and will only include such Personal Data that is subject to Privacy Law and provided by the Customer to D&B under the Master Agreement
Personal Data Breach	as defined in Privacy Law
Privacy Law	European Union Regulation 2016/679 and UK GDPR , or other laws recognizing the Standard Contractual Clauses as a legally required and adequate data transfer mechanism, and their implementing legislation, from time-to-time in force in a relevant jurisdiction,
Processor	as defined in Privacy Law
Sub Processor	a third party contracted to process the Personal Data on behalf of D&B.

2. SCOPE

2.1 Except for clause 3.1 and Schedule 5 , this DPA applies to personal data which D&B processes as a Processor on behalf of Customer as the Controller.
2.2 The subject matter, duration nature and purpose of the Personal Data provided under this DPA are as specified in the Master Agreement and the type of Personal Data and categories of Data Subject are listed at Schedule 2.
2.3 D&B and Customer shall comply with any changes to this DPA that are necessary under Privacy Law.

3. COMPLIANCE

3.1 Customer will comply with Privacy Law relating to the personal data licensed to Customer by D&B under the Master Agreement, including as the data importer under Schedule 5.
3.2 D&B will comply with Privacy Law relating to the Personal Data, including as the data importer under Schedule 3.
3.3 D&B (i) will only act on documented instructions contained within the Master Agreement regarding the processing of Personal Data, (ii) will not process Personal Data for any purposes other than for the purpose(s) specified in the Master Agreement, (iii) will not disclose Personal Data to any third party unless requested to do so by Customer or required by law. D&B shall notify Customer if it believes that the instructions infringe applicable European Union, European Union Member State or United Kingdom law unless informing Customer is prohibited by law on important grounds of public interest.
3.4 Where disclosure is required by law, D&B will (to the extent permitted bylaw) inform Customer in advance of making the disclosure and will co-operatewith Customer to limit the scope of the disclosure to what is strictly requiredby law.
3.5 Customer represents and warrants that it has all necessary legal rights, title, consents and authority to provide the Personal Data to D&B to process as described herein.
3.6 The parties acknowledge and agree that unless the Master Agreement explicitly states this DPA does not apply, in case of conflict between this DPA and the Master Agreement, the DPA will prevail.

4. CONFIDENTIALITY AND SECURITY

4.1 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 Personal Data) to avoid unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of or damage to Personal Data taking into account the processing and the nature of the Personal Data to be protected.
4.2 D&B will take reasonable steps in regard to the reliability of any of its employees who have access to the Personal Data, including training all such employees in Privacy Law and requiring such employees to maintain confidentiality with respect to the Personal Data. D&B will limit access to the Personal Data (including when in a test environment) to those of its employees who have a business need for access.
4.3 Customer will register and keep up to date in accordance with Schedule 4 the relevant email address(es) of its personnel to receive notifications relating to 4.3(i).
4.4 If D&B becomes aware of a Personal Data Breach, D&B will:
(i) promptly notify Customer of the details of the incident;
(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 Privacy Law including any notifications that Customer is required to make as a result of a Personal Data Breach.

5. COOPERATION

5.1 D&B will delete or return the Personal Data if an account is terminated or not renewed unless European Union, European Union Member State or United Kingdom law requires storage of Personal Data.
5.2 D&B shall make available to Customer information necessary to demonstrate compliance with this DPA and Privacy Law.
5.3 D&B shall implement measures to assist Customer in complying with the rights of the Data Subject
5.4 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 Personal Data. D&B will co-operate with Customer to permit it to respond to such enquiry or complaint.
5.5 D&B shall also assist Customer in relation to (i) any data protection impact assessment or regulatory consultation that Customer is required to make in relation to Personal Data; and (ii) the implementation of technical and organizational security measures as required under Privacy Law.
5.6 D&B will permit Customer to take reasonable steps, and on reasonable notice and during normal business hours, at Customer's cost to assess compliance by D&B with its obligations under this DPA, including by inspecting D&B's data processing facilities, procedures and documentation (limited to a maximum of one (1) inspection in any twelve (12) month period, or such further occasions as may be required by Privacy Law). Customer hereby agrees (i) to limit any inspection to the extent reasonably necessary to confirm such compliance, (ii) to enter into a confidentiality agreement (in a form reasonably acceptable to Customer) in respect of any information that its representative may incidentally be provided access to while carrying out an inspection, (iii) to ensure that Customer's personnel shall comply with all D&B's security policies at the relevant D&B locations and shall always be accompanied by a representative of D&B.

6. SUB-PROCESSORS

6.1 Customer acknowledges and agrees that D&B may use Sub Processors. D&B may continue to use such Sub Processors already engaged by D&B as at the date of this DPA and listed at Schedule 1 (subject to D&B in each case meeting the obligations set out in this DPA).

6.2 Customer will register and keep up to date in accordance with Schedule 4 the relevant email address(es) of its personnel to receive notice of a new Sub Processor (including full details of the processing to be undertaken).

6.3 If on receipt of a notification received under clause 6.2 Customer notifies D&B in writing within 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.

6.4 D&B shall enter into a written agreement or other binding legal act under European Union, European Union Member State or United Kingdom law with each Sub Processor which imposes the same obligations on that Sub Processor as are imposed on D&B under this DPA and the Master Agreement.

6.5 D&B shall remain liable to Customer for any Sub Processor's processing of Personal Data under this DPA and the Master Agreement.

7. INTERNATIONAL DATA TRANSFERS

7.1 To the extent that the processing of Personal Data by D&B and/or any of its Sub Processors involves the transfer of Personal Data to a territory that does not provide an adequate level of protection, the parties undertake to provide appropriate safeguards in accordance with Privacy Law in the form of applicable assessments and a European Union and/or United Kingdom approved data transfer mechanism.

8. GENERAL

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

8.2 In the event that any one or more of the provisions of this DPA shall for any reason be held to be invalid, illegal or unenforceable, the remaining provisions of this DPA 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
Sub Processors

Name	Services	Location
Acxiom	Market Intelligence	US
Amazon Web Services	Cloud storage	US/UK/Ireland/Australia/Singapore
Apteco Limited	Software analytics provider for Market Insight	UK/US
Aronova	IT Services for Portfolio Manager	UK
Bishop Services Inc	Screening Services	US
Cybersoft Inc	IT Services	US
Dun & Bradstreet Inc	Processing Services	US
Dun & Bradstreet Information Services	Processing Services	Ireland
Dun & Bradstreet Ltd	Processing Services	UK
Ensono	Cloud infrastructure and mainframe	US/UK
IBM	Data processors	EU/US/India
Livingston International	Screening services	EU/US
Mendix	Cloud and Software Services	EU
Navisite	Cloud infrastructure service	UK
OKS Group LLC	Business Processing outsourcing	India
Profound	Market Intelligence Services	US
Regulatory Data Corp	Screening Services	US
Steele Inc	Compliance Solutions	US
Vxchange	Data Centre services	US

Schedule 2

Type of Personal Data	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; 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; DUNS Number; type of business; IP address; cookie data; login credentials (username and password); traffic data; images and sounds.
Categories of Data Subjects	Individuals associated or potentially associated with incorporated and unincorporated organisations.

Schedule 3

STANDARD CONTRACTUAL CLAUSES - Module II Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and i.e Customer

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") i.e D&B

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

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.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all

information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

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.[8] 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

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

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 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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[11] 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.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

[11] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the

data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries,

submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[12];

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records orother documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.)

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

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

Data exporter(s):

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

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

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

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

Role (controller/processor):Controller

Data importer(s):

Name: Dun & Bradstreet Inc

Address: 101 JFK Parkway, Short Hills, New Jersey, United States

Contact person's name, position and contact details: Chief Privacy Officer, privacyofficer@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 Order between Controller and Processor, and are signed by virtue of the execution of the Order, and dated as of the effective date of the Order.

Role (controller/processor): Processor

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; 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; DUNS Number; type of business; IP address; cookie data; login credentials (username and password); traffic data; images and sounds.
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 order form

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

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.

D&B safeguards confidential data by using a combination of preventative and detective technologies such as encryption and intrusion detection systems. Alongside these security measures, D&B has policies and procedures in place to validate and enforce controls.

Policies, standards, procedures, and guidelines are a critical component of governance at D&B. They provide the structure and rules around which the organization, and subsidiary organizations operate. The policy set is based partly on the International Organization for Standardization and International Electro Technical Commission (ISO/IEC) 27002 Standard, Information Technology - Security Techniques - Code of Practice for Information Security Controls.

Policies are reviewed and approved on an annual basis by the respective authoring organizations. Revised policies are published on the Company intranet following management's approval, so employees can easily access the policies from their workstations. Significant changes to policies are communicated as necessary via team meetings, security awareness emails and presentations, the company Intranet, and/or companywide email communications. The Chief Information Security Officer (CISO) communicates key policy changes to various steering committees on a quarterly basis. Upon hire, employees are directed to review and acknowledge the Company's policies and procedures on the Company's intranet that set forth D&B's expectations on integrity, security, availability and confidentiality of data.

In addition to policies, D&B also maintains compliance processes that address the processing of protected data to comply with applicable statutory, regulatory, contractual, and security, availability and confidentiality obligations and requirements.

ACCESS MANAGEMENT

The Access Management Policy provides global information security requirements to protect against unauthorized access to data owned by or in the custody of D&B, protect against unauthorized access to computer systems, applications, or operating systems; allow only authorized users the appropriate level of access to the information or portion of the system, application, or operating system necessary to accomplish designated responsibilities, i.e., business need to know; and to help ensure users are accountable for safeguarding their authentication information.

New or Modified User Access

New or modified access to systems and products follow the Access Management Policy. Requests for employee access or modified access to systems and products are initiated through D&B internal request portals. As users may not approve their own requests for access, an approval is required based on the following levels of approvals for:

- The People Team is responsible for approving Standard Users IDs for access to D&B internal network for new hires.
- Manager approval is required for access to D&B internal network, mainframe, and remote access.
- Manager and Asset Owner approval is required for access to applications, servers and databases.
- Manager, Asset Owner, and Global Security & Risk approval is required for access to Root, local administrator, master service accounts, global administrators, and extended access for Service Provider/Vendor accounts.

Manager approval is required to verify that access is appropriate to the user's role in the organization. Asset/Data owner (or delegated steward) approval is required for assigning the level of access granted.

Access rights and privileges necessary to perform a user's job function is granted in accordance with:

- Need to Know
- Need to Use
- Least Privilege
- Segregation of Duties
- Contractual obligations regarding limitation of access to data or services
- Regulatory requirements

Access privileges are granted via a role-based system wherever technically feasible.

Inactive Accounts

Where technically feasible, security administrators lock inactive accounts after a maximum of 60 continuous days of inactivity. Security administrators disable User IDs after a maximum of 90 continuous days of inactivity. Security administrators delete User IDs after a maximum of 120 continuous days of inactivity.

User Access Removal

Upon employee termination, access to the products and systems is revoked upon notification of an employee termination. It is the responsibility of the employee's manager to initiate the official termination by notifying the People Leader who then will terminate the user in the HR system in addition to removing physical access (i.e., access badge, laptop, smartphone). A notification is sent from the HR system to product and system administrators within one business day of a termination. The product and system administrators then disable access to in-scope products and systems, D&B's internal network, remote access, mainframes, and servers. If a manager perceives that a departing employee poses a risk to the security of D&B assets, access to assets is removed immediately rather than on the actual termination date.

In select circumstances, a manager may require access to a terminated user's information assets or data (laptop, email, OneDrive) for business continuity purposes. In these cases, the standard network account is re-enabled with a 30-day account expiry and account ownership is changed to indicate custody of the account has been assigned to another employee. The new account custodian is required to seek additional 30-day extensions if warranted. If access to a business application is required to complete an in-progress transaction, the account may be re-enabled only for the duration of completing the transaction.

User Access Review

Reviews take a combination approach to help ensure users are appropriate and their permissions are appropriate for their job duties. On a periodic basis, internal privileged access reviews are performed by management, and remediation

activities are performed to remove or change access as necessary.

In addition to a review of privileged access, application owners review application IDs which have not been used for greater than 90 days. If a business purpose exists to maintain the account, the account owner provides rationale to the application owner to keep the account active. If rationale is not received, the application owner disables or deletes the account as appropriate.

Authentication

A dictionary of disallowed words including commonly used D&B passwords, words found in the dictionary, common passwords, and common dictionary word variants is maintained and configured on systems to prevent use when setting a password.

Active Directory allows only ten consecutive attempts to enter a valid password. After the threshold has been reached, the ID is locked, requiring the user to:

- wait a minimum of thirty minutes before attempting to log in again, or
- submit a request for a password reset to the security administrator of the system.

System idle timeout is set to lock the user session/workstation after 15 minutes of inactivity. Where lockout is not possible, the user is logged out after 15 minutes of inactivity. Users are required to enter their password to unlock systems after systems are locked manually or through timeout on desktop and server platforms.

Authentication information (passwords, private keys/certificates, and tokens) is communicated via secure methods, e.g., encrypted email. For new hires, authentication information is provided to the hiring manager before the documented start date. Once employment has started, authentication information is only shared with the account owner. Passwords are not stored in clear text and where available, stored as a salted-hash value. Passwords are only transported utilizing protocols and services which employ the use of ways to transfer data which is resistant to eavesdropping, overhearing and tampering.

User and device authentication to information systems is protected by passwords that meet D&B's password complexity requirements.

Multi-Factor Authentication

Multi-factor authentication (MFA) is required for remote sessions and access to environments that host production systems:

- Secure MFA devices such as an MFA OTP (One Time Passcode) device, MFA cryptographic software, or MFA cryptographic device are used.
- Users are authenticated and verified as the authorized user when registering their MFA device/application. Verification processes are documented and maintained by end user operations teams and approved and aligned with Global Security and Risk.
- Users are not able to change their MFA method directly.

NETWORK SECURITY

Network connections are protected through a combination of security controls deemed sufficient for the protection of D&B data and systems with consideration of the applicable data classifications of underlying systems. These are based on the type and purpose of the connection and include, but are not limited to, network segmentation, deployment of firewalls and other security appliances, and appropriate authentication mechanisms.

Access to information available through the network is controlled to prevent and detect unauthorized access while providing secure access to authorized users and systems. All activities and network traffic are logged and centrally stored

using industry standard or vendor specific collection mechanisms.

The implementation of any new networking devices (i.e., routers, switches, firewalls) or components of networking systems follows a formal change management process and is approved by Technology Operations and Global Security & Risk teams. Devices deployed in the D&B network are configured to meet security requirements for their individual purposes (internal, public facing, demilitarized). All non-essential services on network devices are disabled or removed.

Direct public access between public networks (e.g. internet) and any internal D&B network is restricted. Inbound and outbound traffic, from untrusted networks (including guest and external wireless connections) and hosts is restricted.

Connection of a new network to existing corporate or business systems networks at any company location or data center is approved by the security team or follows the standard for VPN tunnel connections. Remote connections to the corporate network are accessed via VPNs and MPLS connections through managed gateways.

Wireless and remote access to outside individuals are identified, inventoried, and managed.

DATA SECURITY

Data owners classify data based on definitions defined by Enterprise Data Governance. Access to update data classifications is limited to authorized data owners. Data classification considerations include confidentiality of data, and changes to data classifications are documented and approved. Management determines the treatment of data according to its designated data classification level.

For each classification, several data handling requirements are defined to appropriately safeguard the information. The overall sensitivity of D&B data encompasses security, confidentiality, integrity, and availability of data.

In addition to standard safeguards, particularly sensitive data is provided additional levels of security:

- Sensitive data stored within the trusted private network boundaries of D&B, Symmetric encryption is used, and/or the data may be tokenized, obfuscated or sanitized. Sensitive, data stored in public untrusted networks, Asymmetric Encryption is used, and/or the data may be tokenized, obfuscated or sanitized. Sensitive data stored in IaaS, PaaS, SaaS storage, is encrypted and/or sanitized, obfuscated or tokenized of sensitive data within D&B network trusted boundaries prior to movement of data.

- Sensitive data is not permitted on the end user systems.

- Any non-public data is only made externally accessible via secure transportation channels. Internal use data is not made externally accessible unless there is appropriate authorization from the business and data owner. Internal Use Only data is only accessible to authorized users based on “need-to-know” and least privilege basis.

All data, regardless of classification, stored on removable media (CD, DVD, USB memory sticks, hard drives, etc.) is encrypted using symmetric encryption. Where Cloud Provider's configuration permits for PaaS and SaaS services, encryption is used.

For new applications or existing applications undergoing major changes architecture reviews are performed by the Global Security and Risk team. Major changes are defined as a significant infrastructural change or a change to data sources or business logic.

DETECTION AND RESPONSE

D&B investigates security, availability and confidentiality events and responds to any real or suspected breach of security

of D&B information systems in a timely, coordinated fashion while complying with applicable laws and regulations.

The CISO has designated an Information Security Incident Response Team (IRT) who is responsible for overall Incident response strategy including planning, development, acquisition, implementation, testing, training, and maintenance around the Incident Response Policy and Plan. Personnel on the Incident Response Team are trained in their Incident response roles and responsibilities.

In addition, all employees and contractors are responsible for understanding and reporting potentially adverse Events; therefore, D&B informs and provides educational materials to all employees and contractors pertaining to Incident response, reporting, and procedures. D&B employees and contractors are required to report suspected Security Events to designated channels as soon as they observe the Event(s). In addition, Customers or Third Parties who identify suspected Security Events, including events related to availability or confidentiality, are provided mechanisms to report these suspected Events securely to D&B.

D&B has developed and maintains practices which establish Information Security Incident classification and prioritization based on the severity of the Incident and the sensitivity of affected systems and data. To support these efforts, D&B has implemented and monitors alerts from various tools (i.e., IDS/IPS, SIEM, Firewalls, Web Proxies, etc.) to provide an effective detection capability. Investigation of alerts and Security Events, including events related to availability and confidentiality, are conducted to detect new attack patterns as quickly as possible and incidents declared based on the outcome of the investigation. A register of Security Events is maintained, along with their severity and relevant reporting on the Event.

D&B maintains an Incident Response Plan that provides the company with a roadmap for implementing its Incident Response capability and details the incident management actions. Alerts and reported Security Events are assessed and Security Incident declarations are made by the CISO, or authorized delegate. The Incident Response Plan is activated upon the declaration of an Incident. Security Incident response procedures are conducted and carried out as specified within the Incident Response Plan. An incident communication plan is formally documented and is disclosed in accordance with the Incident Response Plan. The Incident Response Plan and supporting procedures are updated based on lessons learned activities, changes in the evolving threat landscape, when new tools/processes are introduced and/or to address system/organizational changes. The Incident Response Plan is distributed and communicated to the appropriate teams when any updates are made. The Incident Response Plan is reviewed and tested at least annually or upon request by the CISO.

Monitoring tools are in place to measure current usage against predefined thresholds and generate alerts to notify application and infrastructure support teams when thresholds are exceeded. Alerts are reviewed to determine if corrective action is required. In the event additional information assets are required to address usage needs, they will be deployed in accordance with formal asset deployment and change management policies.

Senior operations management reviews the capacity report for applicable information assets and proposes adjustments to capacity based on need and actual usage. Changes to capacity are processed through the D&B standard change management process.

Audit logs are configured to record significant information security-relevant activities and events in the D&B systems. When Information systems or devices are being selected or developed for use with D&B, the logging and monitoring rules are included as information security requirements.

The minimum retention period for log files is one year. The Technology Owner determines whether logs need to be retained for a longer period, based on a risk assessment that takes in to account audit, legal and regulatory, evidentiary or other requirements. Monitoring is in place to help ensure storage capacity needs are sufficient.

SYSTEM SECURITY

D&B has implemented and uses a single, enterprise-wide IT asset management process and management system to actively track and manage computing assets throughout their lifecycle. The IT hardware asset class includes:

- Server Assets, such as physical or virtual servers, and cloud platform instances
- Workstation Assets, such as desktop computers, laptops, notebooks or tablets

Assets are registered, tagged and named using a naming convention that is standard globally within D&B. Upon setup, the computer is registered in the corporate electronic registry to make asset information retrieval possible.

The Global Technology and Asset Management team monitor servers, workstations and portables, including IaaS (cloud) environments, using inventory discovery agents. Discovery will inventory all hardware and software present on those systems and determine whether the organization has all required licenses.

Server or workstation assets will retire only when formal decommissioning processes have been completed:

- Decommissioned Asset Data Archive - Records for assets approved for decommissioning are retained in the asset management system, then moved into an archive database within the asset management system.
- Persistent Data Handling - Upon completion, decommissioned assets are authorized to have their persistent data storage devices removed (if removable). These devices are transferred to either legal hold or disk destruction before the asset can be approved for disposal.
- Repurposing Hardware Assets - A decommissioned physical server may be repurposed for future use if the server model has not reached its own end-of-life status. A persistent data storage device can also be repurposed provided it has been wiped.
- Decommissioning Virtual Servers - A decommissioned virtualized server (VM) follows the same decommissioning process as a physical server before the VM instance can be deleted. The VM's data record is archived within the asset management system.

D&B information on persistent data storage devices is rendered unrecoverable, so that the information cannot be read or reconstructed without unreasonable time or cost. The process of making the data unrecoverable has two primary components, data destruction and storage device destruction. Both are performed if applicable as described below when decommissioning a hardware asset.

- Data Destruction - Before a device is redeployed, the data on it is destroyed by "wiping" to prevent its retrieval.
- Device Destruction - If a persistent data storage device is not being redeployed, and is not subject to Legal Hold, once the decommissioning process for it is complete, it is physically destroyed. In the U.S., this is performed by preauthorized third-party providers who are certified by the National Association for Information Destruction (NAID) for AAA destruction service. Physical destruction is accomplished by "shredding" or "drilling" the device.
- Work Location and Certification
    - Data destruction is performed on-site, and a certificate of destruction delivered.
    - Storage device destruction is either performed on-site or off-site. If conducted off-site, a certificate of destruction is provided back to D&B within the contracted time.

Use of removable electronic media (such as USB drives) is restricted by disabling the USB ports on machines. Business justification and direct manager approval is required to have the USB port enabled. When no longer needed, users submit a ticket to the service desk to have the USB port disabled.

Laptops are protected by encryption. Anti-malware software is implemented and maintained across platforms (workstations and servers) that are susceptible to compromise.

The Global Security and Risk team provides common security configurations which provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. Sources of industry-accepted system configuration standards may include, but are not limited to:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)

- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

The baseline configuration standards help ensure an information system is consistent with enterprise architecture. Product versions of security related technologies are set to either N (current) or at N-1 and kept up to date by applying the latest security patches.

All changes to configurations are made through a formal change control process and include Documentation of impact; Change approval by authorized parties; Functionality and security testing; Back out or reversal plan; Updates to the configuration management repository

Configuration Standards are reviewed annually and updated as follows:

- When required due to system upgrades, patches, or other significant changes have occurred in the baseline configuration
- As an integral part of information system component installations and upgrades
- When an increase in interconnection with other systems outside the authorization boundary or significant changes in the security requirements for the system

In cases where a baseline configuration standard does not exist for an operating system, the Global Security and Risk team helps ensure a baseline security configuration is developed, documented and approved.

Security reviews are conducted on configuration baselines periodically to help ensure compliance and that vendor recommendations and industry best practices are considered.

Malicious code protection mechanisms are deployed at information system entry and exit points on the network to detect and eradicate malicious code that is: transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or inserted through the exploitation of information system vulnerabilities.

Malicious code protection mechanisms (including signature definitions) are updated whenever new releases are available.

All malicious code protection mechanisms are configured to:

- Perform periodic scans of information systems and real-time scans of files from external sources as the files are downloaded, opened, or executed
- Block malicious code, quarantine malicious code, and send alerts to administrator in response to malicious code detection.
- Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Malicious code protection mechanisms are enabled to automatically update and prevent non-privileged users from circumventing malicious code protection capabilities.

VALIDATION AND TESTING

Change Management

Changes to Information assets and systems undergo formal change management review and approval process prior to any implementation in the production environment. The following are considered as part of change management process:

- Risk impact;
- Change approval by authorized personnel;
- Functionality and security testing~~;~~
- Implementation, Testing and Backout plans;
- Updates to the configuration management repository

Vulnerability Management

The D&B Vulnerability Management process consists of three key steps:

- Monitoring & Awareness
- Assessment & Classification
- Mitigation & Remediation

The Global Security and Risk (GSR) Vulnerability Management team is responsible for all infrastructure vulnerability and compliance scanning across the D&B environment. This includes:

- continuous scanning to monitor for new threats and vulnerabilities;
- assessment of external and internal threats from identified vulnerabilities;
- review and report findings to proper asset owners;
- assist with remedial actions within a timeframe appropriate to the risk and threat;
- escalate and manage oversight for critical vulnerabilities, and
- conduct ongoing compliance scanning for compliance with configuration baselines

Scanning occurs at different times and cadences depending on the specific environment and needs. Scanning is performed from locations both inside and outside of the D&B network by commercially available scanning tools.

All identified threats and vulnerabilities are assigned a risk ranking of Critical, High, Medium or Low and action plans are implemented to remediate or mitigate the risk.

The Vulnerability Management (VM) team reviews all results from each scan to validate the accuracy of each finding and removes any false positives. Upon completion of the review, the VM team generates a report of the findings, if requested.

The open findings are communicated to D&B Technical Operations and Application Owners for remediation via D&B's ticket management system. Remediation status is tracked via D&B's ticket management system.

Vulnerabilities remain in an open status until remediated. Tickets are closed, and vulnerabilities are considered remediated only after the VM Team validates the effectiveness of the remediation, either through manual or automated testing. If remediation cannot occur within the established SLA's, the owner of the vulnerability must provide rationale and accept the risk of the open vulnerability.

Monthly, the status of the open vulnerabilities is communicated to various stakeholders by the Chief Information Security Officer and Director of Vulnerability Management.

SOFTWARE SECURITY

The security of D&B software and applications is assessed through the application vulnerability management program.

Application scanning is performed on both application source code and the live applications to identify security vulnerabilities. The primary focus is on (but not limited to) identification of Open Web Application Security Project (OWASP) Top 10 issues:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control

- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Invalidated Redirects and Forwards

The scanning process uses a variety of tools to find issues. The output of the process is an Application Penetration Test report that is produced by the Application Security team. The report documents issues, assigns a severity rating, and identifies the required timeframe for remediation (based on the severity of the issue). All issues rated medium and above are logged in the central ticketing repository for tracking purposes.

The static code analysis (SAST) is performed against an approved and accessible source code management system. The static code analysis tool analyzes a code repository against a scan engine that consists of multiple rule sets. Scan results are available within the Static Code Analysis. The Application Security team assists an application stakeholder in reviewing the results and removes any duplicate and/or false positive findings before publishing to the entire development team.

If the application is externally accessible, the application is enrolled in the Dynamic Application Security Testing (DAST) program for authenticated scanning.

The Application Security team maintains an assessment calendar of the date of the last full penetration test. When an application is nearing its date of the next annual penetration test, the Application Security team contacts the primary application owner. The Application Security team checks to see if the last recorded walkthrough of the application is still valid, and if any major modifications have been made to the application. If a new walkthrough is needed, this is scheduled. Once the testing dates are aligned, the Application Security team determines the type of testing that is needed and schedules this activity. Depending on the application, the test is done via 3rd Party Vendor or an in-house resource. The Application Security team has a closeout call with the application team to walkthrough the findings, the process for remediation, and answer any relevant technical questions. Tickets are created and assigned to the development team for any outstanding findings. Any findings in the scan report are added to the central ticketing repository and tracked against its resolution SLA.

The responsibility for the remediation of identified security vulnerabilities within the specified SLA period lies with the Technical Application Owner. The Application Security team works in partnership with the development teams to support, fix, and test identified vulnerabilities. The Application Security team liaises with the development team to track the progress of the remediation of vulnerabilities. If third party verification of vulnerability remediation is required, this is arranged by the Application Security team.

Developers do not deploy code or modify binaries on the production environment; changes to the production environment are performed through the change and release management.

AWARENESS AND TRAINING

Preventing information security incidents requires users to be aware of security threats and to act appropriately in both defending networks and identifying threats. Awareness and training activities include user-appropriate training and fostering a culture of information security within the organization.

At D&B, security is everyone's responsibility and we understand it all starts with our employees. We continuously train and reinforce security best practices to keep employees up-to-date with the latest information they need to keep our company, and your data, secure. D&B has a formal security awareness and training policy that is available via the Intranet and made available to all employees and contractors. This policy addresses purpose, scope, roles, responsibilities, and management commitment. D&B maintains and provides security awareness training to all information system users on an annual basis

D&B Team Members and contractors complete security awareness training, which includes updates about relevant policies and how to report security events to the authorized response team.

Phishing simulations are performed periodically to test user awareness related to newly identified phishing attempts. Repeat offenders are provided additional communication and training support to make them aware of common pitfalls around Phishing and methods to avoid attacks.

Employees that materially fail to comply with D&B policies are subject to a disciplinary process.

BUSINESS CONTINUITY MANAGEMENT

The goal of Business Continuity Management (BCM) is to identify potential threats to the business, understand their impacts and develop continuity strategies and plans for mitigation. Business continuity strategies and plans have been developed to address events such as natural disasters (significant weather storms, hurricanes, pandemics, etc.) and manmade disasters (political unrest, terrorism, technology issues etc.).

The Business Continuity Management (BCM) Team assists with the global planning, preparedness and training for business continuity at D&B. The BCM Team provides guidance and oversight for global business continuity management.

D&B uses Disaster Recovery Institute International (DRII), Business Continuity Institute (BCI) guidelines based on the ISO Standard 22301 and industry best practices as the guiding principles and structure for its BCM program. Each business unit has an assigned Business Continuity Coordinator (BCC) who liaise between the business unit and the BCM Team to complete Business Impact Analysis (BIA's), Business Continuity Plans (BCP's) and coordinate testing. Business Continuity plans are tested annually via table top exercises. After action reports are completed upon the completion of the testing and results are shared with the BCC team. Additionally, emergency notification testing is performed, and results communicated.

Dun & Bradstreet's Business Continuity Management System (BCMS) enables stability of our operations following a potential disruption or catastrophic event, such as a natural disaster, pandemic, cybersecurity incident, or other events. The plans within the BCMS define objectives, dependencies, and processes to limit the impact to those with whom we do business.

The Dun & Bradstreet BCMS is governed by a chartered Business Continuity Steering Committee, with expectations summarized in a business continuity policy and a standard operating procedure (SOP). The SOP describes the program activities, required frequencies and responsibilities of the staff in regard to their role. Both governance documents are modeled after ISO 22301. All governance documents are reviewed and updated on an annual basis.

Dun & Bradstreet's business continuity program is comprised of seven key elements: (1) business continuity program structure definition; (2) analysis; (3) strategy identification and implementation; (4) business continuity planning; (5) training and awareness; (6) exercising; and (7) continual improvement. The business continuity lifecycle and management of the program is influenced by:

- Risk treatment priorities
- Organizational objectives and obligations (statutory, regulatory and contractual duties)
- Acceptable level of risk
- Interests of Dun & Bradstreet's stakeholders

Dun & Bradstreet's planning efforts compare business continuity planning outcomes to expectations, assess performance during disruptive incidents, provide management with comprehensive and measurable program performance results, and enable continuous improvement. As such, Dun & Bradstreet:

- Continually reassesses risk, including operational and financial risks, and integrates new risk scenarios into the program;
- Updates business requirements and integrates them into the program;

- Introduces new strategies and technologies as they become available;
- Undertakes quarterly reviews and refines the program based on management direction and business need.

INFORMATION BACKUP

The retention of the backups is determined by their "Backup Tier". Simply put, the Backup Tier is based on the system's classification (Production, Development, QA, Test, etc.). The Backup Tier describes the retention duration for the backup, as well as the media and offsite locations.

THIRD PARTY COMPLIANCE AND VENDOR MANAGEMENT

D&B Third Party Compliance process follows a defined global procurement and risk management lifecycle framework across selection, onboarding, monitoring and termination of the relationship. This includes processes for the assignment of individuals responsible for managing third-party relationships, with procedures for identifying, communicating and resolving issues related to third party vendor services and products.

D&B Third Party Compliance process includes specific requirements for scope of services, roles and responsibilities, compliance, information security privacy commitment and-service level definitions. Third parties must comply with D&B Information Security policies, standards and procedures applicable to the service being provided. Approval and change control processes provide for standard contract language reviews and approval cycles by Legal and Third-Party compliance teams.

Third party vendor contracts include specific requirements for scope of services, roles and responsibilities, compliance requirements, information security requirements, confidential and privacy information management commitment and, and service level definition. Changes to standard contract language is reviewed and approved by the legal and compliance team.

System descriptions that delineate the design and operation of the system, system boundaries, security controls and customer responsibilities are identified, reviewed and made available to customers via master services agreement, the statement of work or customer order.

PHYSICAL & ENVIRONMENTAL SECURITY

Physical access to facilities and secure areas within facilities is provided to authorized personnel only. Asset Owners in coordination with Global Corporate Security determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls effecting associated information security risks. D&B's physical security standards are designed to restrict unauthorized physical access to D&B owned/leased facilities and data centers. The controls include: limited access points, access readers, access monitored by surveillance cameras, and only authorized personnel allowed access.

For D&B's hosted data center providers, the identification, detection and protection mechanism for physical and environmental threats, that could impair the availability of the system components (infrastructure, data, and software), are covered as part of hosting service providers SOC reports for in scope Data Centers and Cloud Platforms hosting D&B's Data Cloud Products and Solutions.

Complementary User Entity Controls (CUEC's) are reviewed to help ensure D&B takes appropriate actions to achieve the control objectives.

Processes are in place to respond to notifications of data center environmental threat events when communicated by our service providers.

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

As above

ANNEX III – LIST OF SUB-PROCESSORS

See schedule 1

Schedule 4

To be notified of any change to our sub processors or of a Personal Data Breach, please register any applicable email addresses at support.dnb.com: Select “My Dun & Bradstreet Subscription, “Mange My Product Notifications”, “Create User” (or “Log In”), then go to the “Legal & Contractual” tab and select “Change of Sub Processors” or “Security Incident as per Contract” as appropriate.

Schedule 5

STANDARD CONTRACTUAL CLAUSES Module 1 – Controller to Controller

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

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.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures

to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

Clause 10
Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[10] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

---

[11] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13
Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[12];

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and

principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

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

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 Inc (represented by D&B Business Information Solutions Unlimited Company)

Address: 101 JFK Parkway, Short Hills, New Jersey, United States (The Chase, Carmanhall Road, Sandyford, Dublin 18)

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 EU 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 Order between Importer and Exporter, and are signed by virtue of the execution of the Order, and dated as of the effective date of the Order.

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 Order that incorporates these Standard Contractual Clauses by reference.

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

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

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

Role (controller/processor):Controller

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; 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; DUNS Number; type of business; IP address; cookie data; login credentials (username and password); traffic data; images and sounds.

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.
n/a

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

Nature of the processing
As outlined in Order

Purpose(s) of the data transfer and further processing
Performance of services pursuant to the Master 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

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