Supplier Data Protection Agreement ("SDPA-C")

Version 21 March 2023

1. Scope, Order of Precedence and Term

_____ ("**Supplier**") is engaged to provide services that include the Processing of Personal Information (as defined below) of Oracle's employees, customers and/or partners ("**Services**") for _____ and/or its ultimate parent company ("**Oracle Corporation**"), and any direct and indirect subsidiaries and affiliates of Oracle Corporation in place as of the Effective Date of this Supplier Data Protection Agreement ("**SDPA-C**") as well as those that succeed to the interest thereof during the term of this SDPA-C (hereinafter referred to as "**Oracle**").

In performing the Services, Supplier shall comply with this SDPA-C which forms an integral part of the underlying services contract by and between Supplier and Oracle ("**Services Contract**"), which together with this SDPA-C, constitutes the parties' ("**Agreement**"). Other than the addition of the changes below, the terms and conditions of the Services Contract shall remain unchanged and in full force and effect; however, this SDPA-C shall replace any prior Supplier Data Processing Agreement or EU Model Clauses between Supplier and Oracle under the Services Contract. In the event of a conflict between (i) the Services Contract or any of the standards and policies referenced in this SDPA-C, and (ii) this SDPA-C, this SDPA-C prevails. Capitalized terms used but not defined herein have the meaning ascribed to them under Applicable Law (as defined below).

2. Data Processing

2.1   The parties acknowledge that the Services may involve the collection and/or use of data, some of which may constitute personal data, personal information, personal identifiable information or equivalent term ("**Personal Information**") as defined under applicable data protection laws and regulations, including the EU General Data Protection Regulation 2016/679 ("**Applicable Law**").

2.2   Supplier and Oracle shall each be responsible for the Processing of Personal Information under their control in the context of Supplier delivering the Services described in the Services Contract. Each party will comply with its respective controller obligations under Applicable Law.

2.3   With respect to Processing Personal Information, Supplier shall, and shall ensure that any person Processing Personal Information on Supplier's behalf shall:

(a)   Process Personal Information only to deliver the Services, and shall not Process Personal Information for any other purpose, unless Supplier obtains Oracle's or the individual's express prior consent for such Processing activities.

(b)   Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and comply, except as otherwise specified by Oracle in the Services Contract, with the Oracle Supplier Information and Physical Security Standards, including any appendices ("**OSSS**") and with the Oracle Supplier Code of Ethics and Business Conduct ("**OSCoE**"). Oracle may update the OSSS and/or OSCoE at its discretion. Supplier shall consult the most recent versions of the OSSS and OSCoE on http://www.oracle.com/corporate/supplier/index.html.

(c) Regularly audit its own business processes and procedures that involve the Processing of Personal Information under the Agreement for compliance with Applicable Law.

(d) Where the Services involve Supplier receiving or collecting Personal Information directly from individuals, Supplier shall provide notice to individuals and obtain consent as required under Applicable Law for the relevant purpose(s).

(e) Unless expressly prohibited by Applicable Law, promptly notify Oracle of any requests for disclosure of Personal Information Processed by Supplier in relation to the Services Contract by law enforcement, state security bodies, or other public authorities.

(f) Promptly take adequate steps to remedy any noncompliance with the Agreement and/or Applicable Law regarding the Processing of Personal Information.

(g) Promptly, but at the latest, within 24 hours of any security incident involving the Services or Personal Information, report such security incidents to Oracle.

(h) Promptly notify and forward to Oracle if an individual submits a request or complaint to Supplier with regards to a Processing activity under the control of Oracle and refrain from responding to the individual's request.

2.4 Where the Services involve a Transfer of Personal Information from:

(a) A member state of the European Economic Area (''EEA") or Switzerland, to a Supplier location outside the EEA or Switzerland that has not received a binding adequacy decision by the European Commission, such Transfers are subject to an unmodified set of the 04 June 2021 EU Controller to Controller Model Clauses (Module 1: Controller to Controller) (or any successor Model Clauses) of which the body and Annex A is incorporated by reference to this Agreement, and the preamble thereto and Annex B are attached (**Annex I**);

(b) The United Kingdom (UK) to a Supplier location outside of the UK that has not received a binding adequacy decision by the Information Commissioner's Office (ICO) such Transfers are subject to an unmodified set of the EU Model Clauses (Module 1: Controller to Controller) (or any successor Model Clauses) of which the body and Annex A is incorporated by reference to this SDPA-C, and the preamble thereto and Annex B are attached (**Annex I**) as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0) (or any successor UK Model Clauses) of which the body is herein attached (**Annex II**) .

(c) Argentina to Supplier located outside Argentina, such Transfers will be governed by an unmodified set of Argentinian Model Clauses of which the body is incorporated by reference to this Agreement, and its Annex A is attached (**Annex III**);

(d) Other jurisdictions subject to data Transfer restrictions, Supplier will implement appropriate Transfer safeguards in accordance with Applicable Law. Supplier will provide Oracle with a copy of the relevant Transfer mechanism and/or related data protection provisions promptly upon request;

If the Supplier Processes Personal Information pursuant to the California Consumer Privacy Act as amended ("**CCPA**"), the terms of the Oracle Supplier CCPA Service Provider Addendum ("**CCPA Addendum**") attached here as **Annex IV**, shall apply. The CCPA Addendum is effective solely to the extent the CCPA applies to Supplier's processing of Oracle Personal Information of natural persons who are residents of California, in Supplier's performance of the Services.

The effective date of this SDPA-C is _____.

Supplier: **Oracle:**

By: _____   By: _____

Name (Print): _____   Name (Print): _____

Title: _____   Title: _____

Signature Date: _____   Signature Date: _____

ANNEX I

Preamble to EU Standard Contractual Clauses for Controller to Controller Transfers
(Module 1) ("Clauses")

1. The unmodified set of the Clauses identified as corresponding to Module 1 in the Implementation Decision adopted by the Commission on June 4th, 2021, of which body is incorporated by reference to this SDPA-C and the annexes herein, applies to the Processing of Personal Information by the Supplier in its role as a Controller as part of the provision of Services under the Agreement, between the Supplier and Oracle, where such Personal Information is Processed by the Supplier and/or a Supplier Affiliate in a third country outside the EU/EEA that has not received an adequacy finding under Applicable European Data Protection Law.

2. Only to the extent applicable with regards to the Processing of Swiss Personal Information, the Parties wish to clarify that (1) references to EU member states in these Clauses shall not be interpreted in such a way that data subjects in Switzerland are excluded from exercising their rights at their habitual residence in Switzerland, (2) these Clauses also protect data pertaining to legal entities as long as the Swiss Federal Act of 19 June 1992 on Data Protection, as amended, including the Ordinance to the FADP, remain in force; and that (3) the Swiss Regulator is the competent authority for the purposes of the Agreement.

3. The Parties wish to establish safeguards for their data transfers outside of the EU/EEA and Switzerland in consideration of the Court of Justice of the European Union Schrems II ruling of 16 July 2020 (Case C-311/18), and therefore the body of the Services Contract describes supplementary measures to address such safeguards.

4. The parties agree to the following modifications in relation to the body of the Clauses:

    • The agree to use option 1 identified under section 17 of the Clauses and further chose Ireland as governing law for the Clauses.

    • The parties agree to modify Clause 18 subsection (b) by adding Ireland as choice of forum and jurisdiction.

5. The Clauses apply as of the Effective Date of the Services Contract and will automatically terminate upon the end of the Services Period of the respective Services Contract or until replaced by any other Transfer Mechanism, whichever comes first.

6. The following annexes specified below shall be incorporated and considered part of this Annex I:

    • Annex I.A (Includes the List of Parties, Description of Transfer, and Competent Supervisory Authority)

    • Annex I.B - Technical and organisational measures including technical and organisational measures to ensure the security of the data

Annex I.A

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: the Oracle contracting entity identified in the Services Contract.

Address: the address for the Oracle contracting entity identified in the Services Contract.

Contact person's name, position and contact details:
Refer to Section 3 of the Oracle Services Privacy Policy, available at: https://www.oracle.com/legal/privacy/services-privacy-policy.html#1-6

Activities relevant to the data transferred under these Clauses: the Services as defined in the Services Contract or any applicable Statement of Work (SOW).

Signature and date is effective as of the date of the SDPA-C: Signature and date is effective as of the date of the SDPA-C.

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 Supplier identified in the Services Contract.

Address: the address for the Supplier entity identified in the Services Contract.

Contact person's name, position and contact details: The Supplier contact details are identified in the Agreement and in the absence, the details are set forth below.

Activities relevant to the data transferred under these Clauses: the Services, as defined in the Services Contract or any applicable Statement of Work (SOW).

Signature and date: Signature and date is effective as of the date of the SDPA-C.

Role (controller/processor): **Controller**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Employees, including temporary and prospective employees, relatives, guardians and associates of the data subject, existing and prospective customers, suppliers, visitors or registrants at offices, web sites and/or events, employees of corporate business associates (e.g., resellers of company products and services), advisors, consultants and other professional experts, and/or other categories as set out in the relevant Agreement.

Categories of personal data transferred
Personal contact details including name, home address, home telephone or mobile number, fax number, email address, and passwords, family, lifestyle and social circumstances including age, date of

birth, marital status, number of children and name(s) of spouse and/or children, employment details including employer entity name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details, results from background checks, administrative, audit, accounting and financial information, including tax information and bank details, information gathered in connection with investigations such as video footage and ID badge records, network, computer, email and phone or other communications or messaging systems, logs, data and files, including network traffic data and domain names of websites visited, emails and files stored in company workspaces, imaging and forensic analysis of computing resources and any data stored on those resources, Personal Information about individuals named in legal matters or correspondence, or provided in connection with the provision of legal, banking, audit and/or financial services, including for conflict checking and billing purposes, financial details, goods and services provided, browser and device information, data collected through automated electronic interactions, application usage data, demographic information, geographic or geo-location information, and/or other data as set out in the relevant Agreement.

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.
Special Personal Information as necessary to perform the Services as more fully described in the relevant Agreement.

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

Nature of the processing
To perform the Services as set out in the Agreement.

Purpose(s) of the data transfer and further processing
To perform the Services as set out in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.
Data will be retained according to the terms of the SDPA and shall be returned or deleted pursuant to the SDPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.
Strictly for performance of the Services.

C. COMPETENT SUPERVISORY AUTHORITY

The Irish Data Protection Commissioner in accordance with Clause 13 of the Clauses.

ANNEX I.B

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

As set out in the Agreement.

ANNEX II

Preamble to

EU Standard Contractual Clauses for Controller to Controller Transfers
(Module 1) as supplemented by the UK International Data Transfer Addendum ("UK Clauses") in accordance with the UK GDPR and UK Data Protection Act

1. An unmodified set of the Clauses annexed to the Implementation Decision adopted by the Commission on June 4th, 2021 for the transfer of personal information to third countries pursuant to Regulation (EU) 2016/679, as supplemented with the UK's International Data Transfer Addendum (version B1.0) (or any successor UK Model Clauses) ("UK Addendum" and collectively, the "UK Clauses") applies to the Processing of Personal Information by the Supplier in its role as a Controller as part of the provision of Services under the Agreement, between the Supplier and Oracle, where such Personal Information is Processed by the Supplier and/or a Supplier Affiliate in a third country outside the United Kingdom that has not received an adequacy finding from the ICO or another competent UK Regulator of Oracle acting as a data exporter to the Supplier acting as data importer.

2. The Parties wish to clarify that

   (i) The content required in Tables 1 and 3 of the UK Addendum shall correspond to the respective content in the annexes of the EU Clauses, as supplemented by the Services Contract.

   (ii) The selectable and optional provisions agreed set out in the Preamble to the Clauses shall be mirrored into Table 2 of the UK Addendum.

   (iii) The UK Clauses shall be governed by the laws of England and Wales.

   (iv) The Mandatory Clauses of the UK Addendum shall automatically be incorporated into the Services Contract.

   (v) The following annexes shall be incorporated and considered part of this Annex II:

      • Annex I.A (Includes the list of Parties, Description of Transfer, and Competent Supervisory Authority)

      • Annex I.B - Technical and organisational measures including technical and organisational measures to ensure the security of the data

      • The below International Data Transfer Addendum to the EU Commission Standard Contractual Clauses.

This Addendum does not need to be completed

ORACLE®

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Effective Date of this SDPA-C	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: **The Oracle contracting entity identified in the Services Contract.** Trading name (if different): Main address (if a company registered address): **The address for the Oracle contracting entity identified in the Services Contract.** Official registration number (if any) (company number or similar identifier):	Full legal name: **The Supplier identified in the Services Contract** Trading name (if different): Main address (if a company registered address): **The address for the Supplier identified in the Services Contract** Official registration number (if any) (company number or similar identifier): **The official registration number for the Supplier identified in the Services Contract**
Key Contact	Full Name (optional): **Refer to Section 3 of the Oracle Services Privacy Policy, available at: https://www.oracle.com/legal/privacy/services-privacy-policy.html#1-6**	Full Name (optional): **Unless defined in this SDPA-C, the Supplier contact details are identified in the Services Contract**

	Job Title: ▨	Job Title: ▨
	Contact details including email: ▨	Contact details including email: ▨
Signature (if required for the purposes of Section (2	**Signature and date is effective as of the date of the Services Contract**	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: ▨ Reference (if any): ▨ Other identifier (if any): ▨ Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	Controller to Controller	X	Not applied			
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As described under Annex I to the Clauses included above under this SDPA-C

Annex 1B: Description of Transfer: As described under Annex I.A to the Clauses included above under this SDPA-C

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described under Annex I.B. to the Clauses included above under this SDPA-C

Annex III: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table .3
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4.   This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5.   If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6.   If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7.   If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8.   Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy
9.   Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10.   Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except

where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

   a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

   b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

   c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

   a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

   b. In Clause 2, delete the words:

      "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";

   c. Clause 6 (Description of the transfer(s)) is replaced with:

      "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

   d. Clause 8.7(i) of Module 1 is replaced with:

      "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

   e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

      "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

   f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a   its direct costs of performing its obligations under the Addendum; and/or

    b   its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

ANEXO A	ANNEX A
DESCRIPCIÓN DE LA TRANSFERENCIA	**DESCRIPTION OF THE TRANSFER**

Ver la Descripción de la Transferencia adjunta para detalles sobre la naturaleza y categorías de los datos a transferir, detallando los mismos, la finalidad del tratamiento al que serán sometidos.

Please refer to the attached Annex I

Forma en que se atenderán los pedidos del titular del dato o la autoridad

How requests from the data subject or the authority will be addressed:

El importador de datos notificará al exportador de datos, con excepción de aquellos casos en los que la Ley aplicable al importador de datos lo prohíba específicamente, de cualquier tipo de requerimiento que éste reciba por parte de una persona o agencia de protección de datos con relación a datos personales procesados. El importador de datos cooperará con el exportador de datos con respecto a cualquier acción relacionada con dicho requerimiento.

Data Importer will promptly notify Data Exporter, unless specifically prohibited by laws applicable to Data Importer, if Data Importer receives any requests from an individual or a data protection authority with respect to Personal Information processed. Data Importer will cooperate with Data Exporter with respect to any action taken relating to such request.

La jurisdicción en la que se radicarán los datos:
Los datos personales transferidos serán almacenados en **la jurisdicción donde el importador de datos esté localizado, tal y como consta en las páginas de firma de este Contrato | cualquier jurisdicción donde los afiliados o proveedores de servicios del exportador e importados de datos estén localizados**.

Jurisdiction where the data are to be stored:
The personal data transferred will be stored in **the jurisdiction where the Data Importer is located, as identified in the signature pages of this Agreement | any jurisdiction in which the affiliates or service providers of the Data Exporter and Data Importer may be located**.

Data Importer

By:
_____

Name:

Company:

Title:

Address and Country of Establishment:

_____

_____

ANNEX IV

Oracle Supplier CCPA Service Provider Addendum

This Oracle Supplier CCPA Service Provider Addendum ("**CCPA Addendum**") amends the Agreement between the Supplier and Oracle. The parties agree to amend the Agreement to address the California Consumer Privacy Act as amended (collectively the "**CCPA**") as follows:

1. Capitalized terms used and not defined herein have the meaning(s) given to them in the Agreement. In the event of any conflict between this CCPA Addendum and the Agreement, the terms of this CCPA Addendum prevail.

2. The terms "Business Purpose", "Personal Information", "Sensitive Personal Information", "Sale", "Share", and "Service Provider" have the meanings ascribed to them in the CCPA. In this CCPA Addendum, the term Personal Information includes Sensitive Personal Information.

3. The Supplier is a Service Provider in performing the Services under the Agreement. Supplier will not:
   a. Sell or Share any Personal Information;

   b. retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Agreement, including for any commercial purpose, or (ii) outside of the direct business relationship between the Supplier and Oracle; or

   c. combine Personal Information received from or on behalf of Oracle with Personal Information received from or on behalf of any third party, or collected from Supplier's own interaction with individuals or data subjects, except to perform a Business Purpose that is permitted by the CCPA and the Agreement.

4. The parties acknowledge that the Personal Information Oracle discloses to the Supplier is provided only for the limited and specified purposes set forth in the Agreement. The Supplier shall provide the same level of protection to Personal Information as required by the CCPA and as more fully set out in the Agreement.

5. Oracle may take such reasonable steps as may be necessary (a) to remediate Supplier's unauthorized use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this CCPA Addendum and the Agreement.

6. Supplier shall immediately notify Oracle if it is not able to meet the requirements under this CCPA Addendum.

7. This CCPA Addendum shall not change any of the other rights, obligations, and terms under the Agreement. Subject to the modifications herein, the Agreement shall remain in full force and effect.