

# Data Processing Addendum





## PULSANT DATA PROCESSING ADDENDUM

This Data Processing Addendum (**DPA**) supplements the Pulsant General Terms and Conditions available at <https://www.pulsant.com/terms-and-conditions> or the Pulsant Master Services Agreement, as updated from time to time or as otherwise agreed between Pulsant and Client (**Master Agreement**), governing Client's use of the Services (as defined in the Master Agreement). Unless otherwise defined in this DPA or in the Master Agreement, all capitalised terms will have the meaning given to them in Clause 1 of this DPA.

### 1 DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this DPA.

#### 1.1 Definitions:

**"Business Purposes"** means the services to be provided by Pulsant to the Client as described in the Master Agreement and any other purpose specifically identified in Appendix A.

**"Commissioner"**: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

**"Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing"**: have the meanings given to them in the Data Protection Legislation.

**"Client Data"** means the Personal Data uploaded by the Client for the purposes of using the Services.

**"Data Protection Legislation"**: means

- (a) to the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data;
- (b) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Client or Pulsant is subject, which relates to the protection of Personal Data; and
- (c) any other data protection or privacy laws of any other country applicable to any of the parties.



**“Data Subject”** means the identified or identifiable living individual to whom the Personal Data relates.

**“EU GDPR”** means the General Data Protection Regulation ((EU) 2016/679).

**“EEA”** means the European Economic Area.

**“Standard Contractual Clauses”** or **“SCCs”** means:

- (a) to the extent the UK GDPR applies, the UK Addendum; and/or
- (b) to the extent that the EU GDPR applies, the European Commission’s Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 (as amended in line with the options set out in the UK Addendum forming Appendix B);

**“Term”**: this DPA’s term as defined in Clause 9.

**“UK Addendum”** means the International Data Transfer Addendum to EU Standard Contractual Clauses issued by the ICO under section 119A(1) of the Data Protection Act 2018, version B1.0, in force 21 March 2022 and any updates or replacements as may be issued by the ICO from time to time in accordance with section 119A(1), a copy of which forms Appendix B.

**“UK GDPR”**: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this DPA.

1.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA.

## **2 NATURE, SCOPE AND PURPOSE OF THE PROCESSING**

2.1 This DPA applies when Client Data is Processed on behalf of the Client by Pulsant. In this context, Pulsant will act as a Processor to the Client, who may act as a Controller or Processor of the Client Data.

2.2 Pulsant shall only Process Client Data in accordance with the Client’s instructions and to the extent necessary for providing the Services, as described in the Master Agreement.



- 2.3 Appendix A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types which Pulsant may process Client Data to fulfil the Business Purposes.

### **3 PULSANT'S OBLIGATIONS**

- 3.1 Pulsant will only process the Client Data to the extent, and in such a manner, as is necessary for the Business Purposes and otherwise in accordance with the Client's written instructions. Pulsant will not process the Client Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. Pulsant will promptly notify the Client if, in its opinion, the Client's instructions do not comply with the Data Protection Legislation.
- 3.2 Pulsant will maintain the confidentiality of the Client Data and will not disclose it to third parties unless the Client or this DPA specifically authorises the disclosure, or as required by applicable law, court or by a regulator (including the Commissioner). If applicable law, court or a regulator (including the Commissioner) requires Pulsant to process or disclose the Client Data to a third party, Pulsant will, where possible, inform the Client of such legal or regulatory requirement and give the Client an opportunity to object or challenge the requirement, unless applicable law prohibits the giving of such notice.
- 3.3 Pulsant will reasonably assist the Client with meeting the Client's compliance obligations under the Data Protection Legislation, taking into account the nature of Pulsant's processing and the information available to Pulsant, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner under the Data Protection Legislation. For the avoidance of any doubt, the Client will be solely responsible for responding to Data Subject access requests and Pulsant will instruct any Data Subject to contact the Client if Pulsant receives a Data Subject access request directly.
- 3.4 Pulsant shall notify the Client of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting Pulsant's performance of the Master Agreement or this DPA.

### **4 SECURITY**

- 4.1 Pulsant shall at all times implement the technical and organisational measures against unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Client Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data, as set out in Appendix C.



## 5 PERSONAL DATA BREACH

- 5.1 Pulsant will notify the Client without undue delay if it becomes aware of:
- 5.1.1 the loss, unintended destruction or damage, corruption, or usability of part or all of the Client Data. Client will be responsible for carrying out appropriate back-ups and archiving and for restoring any lost or damaged Client Data.
  - 5.1.2 any accidental, unauthorised or unlawful processing of the Client Data; or
  - 5.1.3 any Personal Data Breach.
- 5.2 Where the Pulsant becomes aware of (a), (b) and/or (c) above, it shall, without undue delay, also provide the Client with the following information:
- 5.2.1 description of the nature of (a), (b) and/or (c), including the categories of in-scope Client Data and approximate number of both Data Subjects and the Client Data records concerned;
  - 5.2.2 the likely consequences; and
  - 5.2.3 a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.
- 5.3 Immediately following any accidental, unauthorised or unlawful Client Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter.
- 5.4 Pulsant will not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Client Data and/or a Personal Data Breach without first obtaining the Client's written consent, except when required to do so by domestic law.
- 5.5 Pulsant agrees that the Client has the sole right to determine:
- 5.5.1 whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Client's discretion, including the contents and delivery method of the notice; and



5.5.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

5.6 Pulsant will cover all reasonable expenses associated with the performance of the obligations under Clause 5.1 to Clause 5.3 unless the matter arose from the Client's instructions, negligence, wilful default or breach of this DPA, in which case the Client will cover all reasonable expenses.

## **6 CROSS-BORDER TRANSFERS OF PERSONAL DATA**

6.1 Other than where the transfer is to an approved Subcontractor referred to at Clause 7 below, Pulsant (and any subcontractor) will not transfer or otherwise process the Client Data outside the UK/EEA without obtaining the Client's prior written consent. Such consent is not to be unreasonably withheld or delayed.

6.2 Where such consent is granted or the Subcontractor is otherwise approved, Pulsant shall process, or permit the processing, of the Personal Data outside the UK/EEA under the following conditions:

6.2.1 Pulsant is processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; or

6.2.2 Pulsant participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that Pulsant (and, where appropriate, the Client) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR and EU GDPR.

6.3 If any Client Data transfer between the Client and Pulsant requires execution of SCCs in order to comply with the Data Protection Legislation (where the Client is the entity exporting Personal Data to Pulsant outside the EEA), the parties shall be deemed to have executed, the SCCs/ contained in Appendix B, and take all other actions reasonably required to legitimise the transfer.



## **7 SUBCONTRACTORS**

- 7.1 Those subcontractors approved as at the commencement of this Agreement are as set out in Appendix A.
- 7.2 Prior to Pulsant engaging a new sub-contractor, Pulsant shall: (a) notify Client by email to Client's designated contact(s); and (b) ensure such sub-contractor has entered into a written agreement with Pulsant (or the relevant Pulsant Affiliate) requiring the sub-contractor to abide by terms no less protective than those provided in this DPA. The Parties agree that Pulsant will be deemed to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

## **8 COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS**

- 8.1 Pulsant shall make available such technical and organisational measures as may be appropriate, and promptly provide such information to the Client as the Client may reasonably require, to enable the Client to comply with:
- 8.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
  - 8.1.2 information or assessment notices served on the Client by the Commissioner under the Data Protection Legislation.
- 8.2 Pulsant will notify the Client without undue delay in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Client Data or to either party's compliance with the Data Protection Legislation.
- 8.3 Pulsant will notify the Client within 2 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation. Data Subjects will also be instructed by Pulsant to contact the Client directly.
- 8.4 Pulsant will give the Client all reasonable co-operation and assistance in responding to any complaint, notice or communication from the Commissioner or other regulator.



## 9 TERM AND TERMINATION

9.1 This Agreement will remain in full force and effect so long as:

9.1.1 the Master Agreement remains in effect; or

9.1.2 Pulsant retains any of the Client Data related to the Master Agreement in its possession or control (Term).

9.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Client Data will remain in full force and effect.

## 10 DATA RETURN AND DESTRUCTION

10.1 At the Client's request, Pulsant will give the Client, or a third party nominated in writing by the Client, a copy of or access to all or part of the accessible Personal Data in its possession or control in the format and on the media reasonably specified by the Client.

10.2 On termination of the Master Agreement for any reason or expiry of its term, Pulsant will securely delete or destroy or, if directed in writing by the Client, return and not retain, all or any of the Personal Data in its possession or control with the exception of any Client data where applicable laws, regulations, or government or regulatory body requires Pulsant to retain any documents or materials or Client Data beyond the term of the Master Agreement.

10.3 Where requested, Pulsant will certify in writing to the Client that it has destroyed the Client Data within 60 days after it completes the deletion or destruction.

## 11 RECORDS

11.1 Pulsant will keep detailed, accurate and up-to-date written records regarding any processing of the Client Data, including but not limited to, the access, control and security of the Client Data, approved subcontractors, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in Clause 4.1 (**Records**).





## **12 AUDIT**

12.1 Pulsant will permit the Client or its third-party representatives to audit Pulsant's compliance with its DPA obligations, on at least 30 days' notice, and no more than once in a 12-month period, during the Term. Pulsant will give the Client or its third-party representatives all reasonable assistance to conduct such audits. The assistance may include:

- 12.1.1 remote electronic access to, and copies of the Records held at Pulsant's premises or on systems storing the Personal Data;
- 12.1.2 access to and meetings with Pulsant's personnel who are reasonably necessary to provide explanations and perform the audit effectively; and
- 12.1.3 details of the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process the Client Data.



## **Appendix A - Personal Data processing purposes and details**

Subject matter of processing: Client Data

Duration of Processing: The Term of the Master Agreement

Nature of Processing: To provide the Services

Business Purposes: the Services

Personal Data Categories:

business contact details (name, email address, business address, business phone numbers) for the purposes of servicing the account

[for cloud services: Application data as controlled by the Client]

Data Subject Types:

Client employees

[for cloud services: Application data as controlled by the Client]

### **Approved Subcontractors:**

All subcontractors as listed at: <https://www.pulsant.com/privacy-policy>

[list other applicable subcontractors]



## Appendix B – International transfer mechanisms

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	The Effective Date of the Master Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Client	Pulsant
Key Contact	See Master Agreement	See Master Agreement
Signature (if required for the purposes of Section 2)	By signing the Agreement the Exporter will be deemed to have signed this Addendum	By signing the Agreement the Importer(s) will be deemed to have signed this Addendum



Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		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	No (Transfer controller to controller)	-	-	-	-	-
2	No (Transfer controller to processor)	-	-	-	-	-
3	Yes (Transfer processor to processor)	Yes	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	OPTION 2: General Written Authorisation	14 days	No
4	Yes (Transfer processor to controller)	Yes	As above	-	-	Yes, potentially.



### **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 per Parties details above

---

Annex 1B: Description of Transfer: as per Appendix A to the DPA

---

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As per Appendix C to the DPA

---

Annex III: List of Sub processors (Modules 2 and 3 only): As listed at: <https://www.pulsant.com/privacy-policy> [and ● ]

---

### **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: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> 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:

<b>Addendum</b>	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
<b>Addendum EU SCCs</b>	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
<b>Appendix Information</b>	As set out in Table 3.
<b>Appropriate Safeguards</b>	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.
<b>Approved Addendum</b>	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.
<b>Approved EU SCCs</b>	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
<b>ICO</b>	The Information Commissioner.



<b>Restricted Transfer</b>	A transfer which is covered by Chapter V of the UK GDPR.
<b>UK</b>	The United Kingdom of Great Britain and Northern Ireland.
<b>UK Data Protection Laws</b>	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.
<b>UK GDPR</b>	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.
-------------------	---



## Appendix C - Security measures

Pulsant has implemented technical and organisational data security measures such as:

### Organisational Measures:

Integrated ISO27001 certified information systems management and associated information security controls and processes, as well as data protection policy and controls. These include staff background checking, regular awareness training and internal audits.

### Technical Measures:

Controls as per Integrated ISO27001 certified information systems management and associated information security controls and processes, as well as data protection controls. These include physical access controls such as access pass-controlled door locks and CCTV, application access controls (including assigned credentials, MFA, access logging), system controls such as firewalls, anti-virus applications, intrusion monitoring and security patching programme.

Client's application data is segregated from other clients. Data is encrypted at rest and in transit. Data stored by Pulsant for the purposes of servicing the Client's account is backed up regularly.